Krishna's

TEXT BOOK on

ADVANCED ALGEBRA

(For B.A. and B.Sc. III[rd] Semester students of Kumaun University)

Kumaun University Semester Syllabus *w.e.f.* 2017-18

By

A.R. Vasishtha
Retired Head, Dept. of Mathematics
Meerut College, Meerut

A.K. Vasishtha
M.Sc., Ph.D.
C.C.S. University, Meerut

Kumaun

KRISHNA Prakashan Media (P) Ltd.
KRISHNA HOUSE, 11, Shivaji Road, Meerut-250001 (U.P.), India

Jai Shri Radhey Shyam

Dedicated

to

Lord

Krishna

Authors & Publishers

Preface

This book on **Advanced Algebra** has been specially written according to the latest **Syllabus** to meet the requirements of **B.A. and B.Sc. Semester-III Students** of all colleges affiliated to Kumaun University.

The subject matter has been discussed in such a simple way that the students will find no difficulty to understand it. The proofs of various theorems and examples have been given with minute details. Each chapter of this book contains complete theory and a fairly large number of solved examples. Sufficient problems have also been selected from various university examination papers. At the end of each chapter an exercise containing objective questions has been given.

We have tried our best to keep the book free from misprints. The authors shall be grateful to the readers who point out errors and omissions which, inspite of all care, might have been there.

The authors, in general, hope that the present book will be warmly received by the students and teachers. We shall **indeed** be very thankful to our colleagues for their recommending this book to their students.

The authors wish to express their thanks to Mr. S.K. Rastogi, *M.D.,* Mr. Sugam Rastogi, *Executive Director,* Mrs. Kanupriya Rastogi, *Director* and entire team of **KRISHNA Prakashan Media (P) Ltd., Meerut** for bringing out this book in the present nice form.

The authors will feel amply rewarded if the book serves the purpose for which it is meant. Suggestions for the improvement of the book are always welcome.

—Authors

Syllabus

ADVANCED ALGEBRA

B.A./B.Sc. III Semester

Kumaun University

Third Semester – First Paper

B.A./B.Sc. Paper-I

Rings: Rings, Various types of rings, Rings with unity, Rings without zero divisors, Properties of rings, Sub rings.

Ideals: Ideals, Quotient rings, Principal ideals, Maximal ideals, Prime ideals, Principal ideal domains, Characteristic of a ring.

Integral Domains and Fields: Integral domain, Field, Skew field etc., Field of quotients of an integral domain, Embedding of an integral domain in a field, Factorization in an integral domain, Divisibility, Units, Associates, Prime and irreducible elements, Unique Factorisation Domain, Euclidean rings.

Polynomial Rings: Polynomials over a ring, Degree of a polynomial, Zero, Constant and monic polynomials, Equality of polynomials, Addition and multiplication of polynomials, Polynomial rings, Embedding of a ring R into R[x], Division algorithm, Euclidean algorithm, Units and associates in polynomials, Irreducible polynomials.

Brief Contents

Dedication.....(v)
Preface.....(vi)
Syllabus (Kumaun University).....(vii)
Brief Contents(viii)

Chapter 1: Rings.....A-01—A-36

Chapter 2: Subrings and Ideals.....A-37—A-82

Chapter 3: Polynomial Rings and Unique Factorization Domain.....A-83—A-140



Krishna's

ADVANCED ALGEBRA

Chapters

1. Rings

2. Subrings and Ideals

3. Polynomial Rings and Unique Factorization Domain

Chapter

1

Rings

1 Ring

So far we have studied group which is an algebraic structure equipped with one binary operation. In this chapter we shall study ring which is an algebraic structure equipped with two binary operations.

Ring:

Definition: *Suppose R is a non-empty set equipped with two binary operations called addition and multiplication and denoted by '+' and '.' respectively i.e., for all $a, b \in R$ we have $a + b \in R$ and $a \,.\, b \in R$. Then this algebraic structure $(R, +, .)$ is called a* **ring** *if the following postulates are satisfied* : **(Kanpur 2005, 07; Bundelkhand 05, 09, 10; Kumaun 08; Gorakhpur 15)**

1. *Addition is associative, i.e.,* $(a + b) + c = a + (b + c) \ \forall \ a, b, c \in R$.
2. *Addition is commutative, i.e.,* $a + b = b + a \ \forall \ a, b \in R$.
3. *There exists an element denoted by* 0 *in* R *such that* $0 + a = a \ \forall \ a \in R$.

4. *To each element a in R there exists an element* $-a$ *in R such that* $(-a) + a = 0$.

5. *Multiplication is associative, i.e.,* $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \forall \ a, b, c \in R$.

6. *Multiplication is distributive with respect to addition, i.e., for all a, b, c in R ,*

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{Left distributive law}$$

and

$$(b + c) \cdot a = b \cdot a + c \cdot a \quad \text{Right distributive law.}$$

Since addition is commutative in R, therefore we shall have $0 \in R$ such that

$$0 + a = a = a + 0 \ \forall \ a \in R.$$

Also if $a \in R$, then we shall have $(-a) + a = 0 = a + (-a)$.

Thus R will be an abelian group with respect to addition. The element $0 \in R$ will be the additive identity. It is called the **zero element** of the ring. Since in a group the identity element is unique, therefore every ring will possess a unique zero element and it will be the identity element for addition composition. We shall always denote this element by the symbol 0.

Students should not confuse it with the number 0. It is a symbol which will represent the additive identity of the ring.

In a ring every element will possess a unique inverse for addition composition. We shall denote the additive inverse of a by the symbol $-a$.

We shall define $a - b = a + (-b)$.

The equation $a + x = b$ will have a unique solution in R and it will be $x = b - a$.

Obviously
$$\begin{aligned} a + (b - a) &= a + [b + (-a)] \\ &= a + [(-a) + b] \\ &= [a + (-a)] + b \\ &= [(-a) + a] + b \\ &= 0 + b = b. \end{aligned}$$

Similarly the equation $y + a = b$ will have a unique solution in R and it will be $y = b - a$.

Both the cancellation laws will hold good for addition in R *i.e.*, for all a, b, c in R

$$a + b = a + c \Rightarrow b = c$$

and
$$b + a = c + a \Rightarrow b = c.$$

If in a ring we have $a + b = 0$, then $a = -b$ and $b = -a$.

Ring with Unity: **(Kanpur 2006)**

If in a ring R there exists an element denoted by 1 *such that* $1 \cdot a = a = a \cdot 1 \ \forall \ a \in R$ *, then R is called a ring with unit element. The element* $1 \in R$ *is called the unit element of the ring.* Obviously 1 is the multiplicative identity of R. Thus if a ring possesses multiplicative identity, then it is a ring with unity.

Commutative Ring: *If in a ring R , the multiplication composition is also commutative i.e., if we have* $a \cdot b = b \cdot a \ \forall \ a, b \in R$ *, then R is called a commutative ring.*

Note: In future we shall denote the multiplication composition in a ring R not by the symbol ' . ' but by multiplicative notation. Thus we shall write ab in place of $a \cdot b$.

2 Elementary Properties of a Ring

Theorem: *If R is a ring , then for all $a, b, c \in R$*

(i) $a0 = 0a = 0$. **(Meerut 2000; Kanpur 07; Gorakhpur 12)**

(ii) $a(-b) = -(ab) = (-a)b$.
(Meerut 2000, 03; 12; Kanpur 07; Bundelkhand 10; Gorakhpur 12)

(iii) $(-a)(-b) = ab$.

(iv) $a(b - c) = ab - ac$. **(Gorakhpur 2011; Meerut 12)**

(v) $(b - c)a = ba - ca$.

Proof: (i) We have

$a0 = a(0 + 0)$ $[\because 0 + 0 = 0]$

$= a0 + a0$. [by left distributive law]

$\therefore$ $0 + a0 = a0 + a0$. $[\because a0 \in R \text{ and } 0 + a0 = a0]$

Now R is a group with respect to addition, therefore applying right cancellation law for addition in R , we get $0 = a0$.

Similarly we have $0a = (0 + 0)a = 0a + 0a$. [by right distributive law]

$\therefore$ $0 + 0a = 0a + 0a$ $[\because 0 + 0a = 0a]$

Applying right cancellation law for addition in R, we get $0 = 0a$.

(ii) We have $a[(-b) + b] = a0$ $[\because -b + b = 0]$

$\Rightarrow$ $a(-b) + ab = 0$ [by using left distributive law and the result (i)]

$\Rightarrow$ $a(-b) = -(ab)$, since in a ring $a + b = 0 \Rightarrow a = -b$.

Similarly we have $(-a + a)b = 0\ b$

$\Rightarrow$ $(-a)b + ab = 0 \Rightarrow (-a)b = -(ab)$,

since in a ring $a + b = 0 \Rightarrow a = -b$.

(iii) We have $(-a)(-b) = -[(-a)b]$, since $a(-b) = -(ab)$

$= -[-(ab)]$, since $(-a)b = -(ab)$

$= ab$,

since R is a group with respect to addition and in a group we have $-(-a) = a$.

(iv) We have $a(b - c) = a[b + (-c)] = ab + a(-c)$ [by left distributive law]

$= ab + [-(ac)]$ $[\because a(-c) = -(ac)]$

$= ab - ac$.

(v) We have $(b - c)\, a = [b + (-c)]\, a = ba + (-c)\, a$ [by right distributive law]
$= ba + [-(ca)] = ba - ca.$

3 Integral Multiples of the Elements of a Ring

Suppose R is a ring and $a \in R$. If m is a positive integer, then we define

$ma = a + a + a + \ldots$ upto m terms.

Also we define $0a = 0$. Here 0 on the left hand side is the integer zero and 0 on the right hand side is the zero element (additive identity) of the ring.

If m is a positive integer, then $-m$ is a negative integer. We define

$(-m)\, a = -(ma) = -(a + a + a + \ldots$ upto m terms$)$

$= (-a) + (-a) + (-a) + \ldots$ upto m terms $= m\,(-a)$.

If m and n are any integers, we can prove that

$ma + na = (m + n)\, a$, $m\,(na) = (mn)\, a$, and $(ma)\,(na) = (mn)\, a^2$.

Also we can prove that for any integer m, we have

$m\,(a + b) = ma + mb \;\forall\; a, b \in R.$

The students should not confuse that this is the distributive law we assumed in the postulates for a ring. It is not so. Here m is an integer and a, b are elements of R.

4 Rings from Number Systems

Illustration 1: *The set R consisting of a single element 0 with two binary operations defined by $0 + 0 = 0$ and $0 \,.\, 0 = 0$ is a ring. This ring is called the null ring or the zero ring.*

Illustration 2: *The set* **I** *of all integers is a ring with respect to addition and multiplication of integers as the two ring compositions. This ring is called the ring of integers.*

(Bundelkhand 2006, 09; Kumaun 06, 11, 13)

As in groups, we should first prove that **I** is an abelian group with respect to addition of integers.

Further we observe that

(i) The product of two integers is also an integer. Therefore **I** is closed with respect to multiplication of integers.

(ii) Multiplication of integers is an associative composition.

(iii) Multiplication of integers is distributive with respect to addition of integers *i.e.*, if a, b, c are any elements of **I**, then

$a\,(b + c) = ab + ac$ and $(b + c)\, a = ba + ca.$

Therefore **I** is a ring with respect to addition and multiplication of integers. The integer 0 is the zero element of this ring. Also the multiplicative identity exists and

it is the integer 1. We have $1a = a = a1 \ \forall \ a \in \mathbf{I}$. Thus the ring of integers is a ring with unity. The integer 1 is the unit element of this ring.

The multiplication of integers is a commutative composition. Therefore it is also a commutative ring.

Illustration 3: *The set* $2\mathbf{I}$ *of all even integers is a commutative ring without unity, addition and multiplication of integers being the two ring compositions.*

Illustration 4: *The set* $\mathbf{Q}$ *of all rational numbers is a commutative ring with unity, the addition and multiplication of rational numbers being the two ring compositions.*

Illustration 5: *The set* $\mathbf{R}$ *of all real numbers is a commutative ring with unity, the addition and multiplication of real numbers being the two ring compositions.*

Illustration 6: *The set* $\mathbf{C}$ *of all complex numbers is a commutative ring with unity, the addition and multiplication of complex numbers being the two ring compositions.*

Illustration 7: *The set* $I_n = \{0, 1, \ldots, n-1\}$ *under addition and multiplication modulo n is a commutative ring with unity 1. The set of units is* $U(n)$. **(Kumaun 2008)**

Illustration 8: *The set* $I[x]$ *of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication is a commutative ring with unity* $f(x) = 1$.

Illustration 9: *The set* $M_2(I)$ *of* 2×2 *matrices with integer entries is a non-commutative ring with unity* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Illustration 10: *The set of all continuous real-valued functions of a real variable whose graphs pass through the point (1, 0) is a commutative ring without unity under the operations of pointwise addition and multiplication, i.e., the operations* $(f + g)(a) = f(a) + g(a)$ *and* $(fg)(a) = f(a)\, g(a)$.

Illustrative Examples

Example 1: *The set M of all* $n \times n$ *matrices with their elements as real numbers (rational numbers, complex numbers, integers) is a non-commutative ring with unity, with respect to addition and multiplication of matrices as the two ring compositions.*

Solution: We know that the sum and product of two $n \times n$ matrices with their elements as real numbers are again $n \times n$ matrices with their elements as real numbers. Therefore M is closed with respect to addition and multiplication of matrices.

Further we observe that

(i) $A + (B + C) = (A + B) + C \ \forall \ A, B, C \in M$, since the addition of matrices is an associative composition.

(ii) $A + B = B + A \ \forall \ A, B \in M$, since the addition of matrices is commutative.

(iii) If O is the null matrix of the type $n \times n$, then $O \in M$ and we have

$$O + A = A \quad \forall \quad A \in M.$$

(iv) To each matrix $A \in M$ there exists a matrix $-A \in M$ such that

$$(-A) + A = O \text{ (null matrix).}$$

(v) $(AB)\,C = A\,(BC)$, $\forall$ $A, B, C \in M$, since multiplication of matrices is associative.

(vi) $A\,(B + C) = AB + AC$,
and $(B + C)\,A = BA + CA$ $\forall$ $A, B, C \in M$, since matrix multiplication is distributive with respect to matrix addition.

Hence M is a ring with respect to the two given compositions. The null matrix O of the type $n \times n$ is the zero element of this ring *i.e.*, $O = 0$.

Since the multiplication of matrices is not in general commutative, therefore the ring is a non-commutative ring. [$n > 1$]

Finally if $\boldsymbol{I}$ be the unit matrix of the type $n \times n$, then $I \in M$ and we have

$$I\ A = A = AI \quad \forall \quad A \in M.$$

Therefore the matrix I is the multiplicative identity.

Thus the ring is with unity and the matrix I is the unity element of the ring *i.e.*, $I = 1$.

Example 2: *The set* $R = \{0, 1, 2, 3, 4, 5\}$ *is a commutative ring with respect to '*$+_6$*' and '*$\times_6$*' as the two ring compositions.*

Solution: As we have proved in groups, we should first prove that R is an abelian group with respect to '$+_6$'.

Now we form the composition table for R for the composition $\times_6$.

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From the composition table we see that R is closed with respect to the composition '$\times_6$'.

Also we know that '$\times_6$' is an associative composition in R *i.e.*,

$$a \times_6 (b \times_6 c) = (a \times_6 b) \times_6 c \ \forall \ a, b, c \in R.$$

Further '$\times_6$' is distributive in R with respect to '$+_6$'. If a, b, c are any elements of R, then

$a \times_6 (b +_6 c) = a \times_6 (b + c)$ $[\because b + c \equiv b +_6 c \pmod 6]$

= least non-negative remainder when $a(b + c)$ is divided by 6

= least non-negative remainder when $ab + ac$ is divided by 6

$= (ab) +_6 (ac) = (a \times_6 b) +_6 (ac)$

$[\because a \times_6 b \equiv ab \pmod 6]$

$= (a \times_6 b) +_6 (a \times_6 c)$ $[\because a \times_6 c \equiv ac \pmod 6]$

Similarly we can prove that

$(b +_6 c) \times_6 a = (b \times_6 a) +_6 (c \times_6 a)$.

$\therefore$ R is a ring with respect to the given compositions. Since '$\times_6$' is a commutative composition in R as is clear from the composition table also , therefore R is a commutative ring. Also 1 is the identity element for the composition '$\times_6$'. Therefore R is a ring with unity. The integer 0 is the zero element of this ring.

Important: We see that in this ring R neither 2 nor 3 is equal to the zero element of the ring. But $2 \times_6 3 = 0$ (zero element of the ring). Thus in a ring it is possible that the product of two non-zero elements is equal to the zero element. Also the number of elements in R is finite. Therefore this is an example of a finite ring.

5 Special Types of Rings: Rings with or without Zero Divisors

We have proved that in any ring R, if 0 is the additive identity *i.e.*, the zero element of the ring, then $0a = a0 = 0 \ \forall \ a \in R$. However there are rings in which it is possible that $ab = 0$ when neither $a = 0$ nor $b = 0$. Such elements are called **zero divisors**.

Definition: *A non-zero element a of a ring R is called a zero divisor or a divisor of zero if there exists an element $b \neq 0 \in R$ such that either $ab = 0$ or $ba = 0$.*

(Kumaun 2006; Kanpur 10)

Ring without zero divisors: *A ring R is without zero divisors if the product of no two non-zero elements of R is zero i.e., if $ab = 0 \Rightarrow a = 0$ or $b = 0$.*

(Meerut 2001; Kumaun 09, 12)

On the other hand if in a ring R there exist non-zero elements a and b such that $ab = 0$, then R *is said to be a ring with zero divisors.* **(Meerut 2003)**

Illustration 1: *Suppose M is a ring of all 2×2 matrices with their elements as integers, the addition and multiplication of matrices being the two ring compositions. Then M is a ring with zero divisors.*

The null matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element of this ring.

Now $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are two non-zero elements of this ring

i.e., $A \neq O, B \neq O$.

We have $AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O.$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring. Therefore M is a ring with zero divisors.

Also it is interesting to note that $BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Thus in a ring R it is possible that $ab = 0$ but $ba \neq 0$.

Illustration 2: *The ring* $(\{0, 1, 2, 3, 4, 5\}, +_6, \times_6)$ *is a ring with zero divisors.*

We have $2 \times_6 3 = 0, 3 \times_6 4 = 0$

i.e., the product of two non-zero elements is equal to the zero element of the ring.

Illustration 3: *The ring of integers is a ring without zero divisors.* The product of two non-zero integers cannot be equal to the zero integer.

Cancellation laws in a ring: If R is a ring then R is an abelian group with respect to addition. For addition composition the cancellation laws hold in all rings. Therefore the question of cancellation laws holding or not in a ring arises only for the multiplication composition.

We say that cancellation laws hold in a ring R if

$$a \neq 0, ab = ac \Rightarrow b = c \quad \text{and} \quad a \neq 0, ba = ca \Rightarrow b = c \text{ where } a, b, c \in R.$$

Theorem: *A ring R is without zero divisors if and only if the cancellation laws hold in R i.e., R is without zero divisors cancellation laws hold in R.*

(Kumaun 2008, 11, 13, 15; Gorakhpur 10, 12, 15)

Proof: First suppose that R has no zero divisors. Let a, b, c be any three elements of R such that $a \neq 0, ab = ac$.

We have $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$.

Since R is without zero divisors, therefore $a(b - c) = 0$ and $a \neq 0 \Rightarrow b - c = 0$ *i.e.*, $b = c$.

Thus the left cancellation law holds in R.

Similarly we can show that the right cancellation law holds in R.

Conversely suppose that the cancellation laws hold in R. If possible let $ab = 0$, $a \neq 0, b \neq 0$.

Then we have $ab = a0$, since $a0 = 0$.

Now $a \neq 0, ab = a0 \Rightarrow b = 0$ by left cancellation law.

Thus we get a contradiction. Hence R is without zero divisors.

6 Integral Domains

Integral Domain: Definition:

A ring is called an integral domain if it (i) is commutative (ii) has unit element, (iii) is without zero divisors. **(Kanpur 2005, 06, 09; Rohilkhand 08; Kumaun 08, 10, 12, 14; Meerut 12; Purvanchal 11; Gorakhpur 15)**

However some authors define an integral domain as a commutative ring without zero divisors. They do not require that an integral domain should definitely possess unit element.

The most important example of an integral domain is the ring **I** of integers. We have proved that **I** is a commutative ring with unity. Also **I** does not possess zero divisors. We know that if a, b are integers such that $ab = 0$, then either a or b must be zero.

Also it can be seen that the algebraic structures (**C, + , .**), (**Q, + , .**), (**R, + , .**) are all integral domains. As an example of a finite integral domain we have the ring $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$.

Inversible Elements in a Ring with Unity: In a ring every element possesses additive inverse. Therefore the question of an element being inversible or not arises only with respect to multiplication.

If R is a ring with unity, then an element $a \in R$ is called inversible, if there exists $b \in R$ such that

$$ab = 1 = ba \text{ . Also then we write } b = a^{-1}.$$

Illustrations:

(i) 1 and – 1 are the only two inversible elements of the ring of all integers.

(ii) $n \times n$ non-singular matrices with real numbers as elements are the only inversible elements of the ring of all $n \times n$ matrices with elements as real numbers.

7 Field

Definition: A *ring R with at least two elements is called a field if it,*

(i) *is commutative,*

(ii) *has unity,*

(iii) *is such that each non-zero element possesses multiplicative inverse.*

(Rohilkhand 2008; Kanpur 05; Bundelkhand 07; Kumaun 08, 10; Meerut 12B; ; Gorakhpur 15)

Illustration 1: *The ring of rational numbers* $(\mathbf{Q}, +, \bullet)$ *is a field since it is a commutative ring with unity and each non-zero element is inversible.*

The rings of real numbers and complex numbers are also examples of fields.

Illustration 2: *The ring of real numbers* $(R, +, \bullet)$ *is a field since it is a commutative ring with unity and each non-zero element is inversible.*

Illustration 3: *The ring of complex numbers* $(C, +, \bullet)$ *is a field since it is a commutative ring with unity and each non-zero element is inversible.*

Illustration 4: *The ring of integers modulo* p. $(I_p, +_p, \times_p)$ *is a field since it is a commutative ring with unity and each non-zero element is inversible.*

Illustration 5: *The ring* $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$ *is a finite field since it is a commutative ring with unity and each non-zero element is inversible.*

If $a, 0 \neq b$ are elements of a field F, then we shall often write

$$ab^{-1} = \frac{a}{b} = b^{-1}\ a.$$

In a field F, we have

$$\frac{a}{b} + \frac{c}{d} = (ab^{-1}) + (cd^{-1}) = (bd)^{-1}\ (bd)\ [(ab^{-1}) + (cd^{-1})]$$
$$= (bd)^{-1}\ [(bd)\ (ab^{-1}) + (bd)\ (cd^{-1})]$$
$$= (bd)^{-1}\ (ad + bc) = \frac{ad + bc}{bd}\cdot$$

[Note that multiplication of F is commutative].

Also
$$\frac{a}{b}\,\frac{c}{d} = (ab^{-1})\ (cd^{-1})$$
$$= (ac)\ (b^{-1}\ d^{-1})$$
$$= (ac)\ (bd)^{-1} = \frac{ac}{bd}\cdot$$

8 Division Ring or Skew Field

(Kumaun 2006, 09, 11, 14)

Definition: *A ring R with at least two elements is called a division ring or a skew field if it* (*i*) *has unity,* (*ii*) *is such that each non-zero element possesses multiplicative inverse.*

Thus a commutative division ring is a field.

Every field is also a division ring. But a division ring is a field if it is also commutative. We shall later on give an example of a skew field which is not commutative *i.e.*, which is not a field.

Theorem 1: *Every field is an integral domain.*

(Meerut 2000, 03; Rohilkhand 07; Kumaun 07, 14; Kanpur 10; Gorakhpur 10)

Proof: Since a field F is a commutative ring with unity, therefore in order to show that every field is an integral domain we should show that a field has no zero divisors.

Let a, b be elements of F with $a \neq 0$ such that $ab = 0$.

Since $a \neq 0$, a^{-1} exists and we have

$$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}\,0$$

$$\Rightarrow \quad (a^{-1}a)\,b = 0 \Rightarrow 1b = 0 \qquad [\because\ a^{-1}a = 1]$$

$$\Rightarrow \quad b = 0. \qquad [\because\ 1b = b]$$

Similarly, let $ab = 0$ and $b \neq 0$.

Since $b \neq 0$, b^{-1} exists and we have

$$ab = 0 \Rightarrow (ab)\,b^{-1} = 0\,b^{-1}$$

$$\Rightarrow \quad a\,(bb^{-1}) = 0$$

$$\Rightarrow \quad a1 = 0 \Rightarrow a = 0.$$

Thus in a field $ab = 0 \Rightarrow a = 0$ or $b = 0$. Therefore a field has no zero divisors. Therefore every field is an integral domain.

But the converse is not true i.e., every integral domain is not a field. For example the ring of integers is an integral domain and it is not a field. The only inversible elements of the ring of integers are 1 and – 1. **(Kanpur 2010)**

Note: For a field unity and zero are distinct elements *i.e.*, $1 \neq 0$. Let a be any non-zero element of a field. Then a^{-1} exists and is also non-zero., we have

$a^{-1} = 0 \Rightarrow aa^{-1} = a0 \Rightarrow 1 = 0 \Rightarrow a1 = a0 \Rightarrow a = 0$ which is a contradiction.

Now a field has no zero divisors. Therefore $1 = a^{-1}\ a \neq 0$.

Remark: A field has no zero divisors. Therefore in a field the product of two non-zero elements will again be a non-zero element. Also the unit element $1 \neq 0$ and each non-zero element possesses multiplicative inverse which is again a non-zero element. The multiplication is commutative as well as associative. Therefore *the non-zero elements of a field form an abelian group with respect to multiplication*.

Theorem 2: *A sfield* (*skew-field*) *has no divisors of zero.*

Proof: Let D be a skew-field. Then D is a ring with unit element 1 and each non-zero element of D possesses multiplicative inverse.

Let a, b be elements of D with $a \neq 0$ such that $ab = 0$.

Since $a \neq 0$, a^{-1} exists and we have

$$ab = 0 \in a^{-1}(ab) = a^{-1}\,0 \Rightarrow (a^{-1}\ a)\,b = 0 \Rightarrow 1b = 0 \Rightarrow b = 0.$$

Similarly, let $ab = 0$ with $b \neq 0$.

Since $b \neq 0$, b^{-1} exists and we have

$$ab = 0 \Rightarrow (ab)\,b^{-1} = 0\,b^{-1} \Rightarrow a\,(bb^{-1}) = 0 \Rightarrow a1 = 0 \Rightarrow a = 0.$$

Therefore a skew-field has no zero divisors.

Theorem 3: *A finite commutative ring without zero divisors is a field.*

Or

Every finite integral domain is a field.

(Meerut 2000, 01, 03, 12, 13B; Kanpur 09; Bundelkhand 09, 10; Kumaun 10, 12)

Proof: Let D be a finite commutative ring without zero divisors having n elements $a_1, a_2, \ldots, a_n$. In order to prove that D is a field, we must produce an element $1 \in D$ such that $1a = a \ \forall \ a \in D$. Also we should show that for every element $a \neq 0 \in D$ there exists an element $b \in D$ such that $ba = 1$.

Let $a \neq 0 \in D$. Consider the n products $aa_1, aa_2, \ldots, aa_n$.

All these are elements of D. Also they are distinct. For suppose that $aa_i = aa_j$ for $i \neq j$.

Then $a(a_i - a_j) = 0.$...(1)

Since D is without zero divisors and $a \neq 0$, therefore (1) implies

$a_i - a_j = 0 \Rightarrow a_i = a_j$, contradicting $i \neq j$.

$\therefore$ $aa_1, aa_2, \ldots, aa_n$ are all the n distinct elements of D placed in some order. So one of these elements will be equal to a. Thus there exists an element, say, $1 \in D$ such that

$a1 = a = 1a.$ [$\because$ D is commutative]

We shall show that this element 1 is the multiplicative identity of D. Let y be any arbitrary element of D. Then from the above discussion for some $x \in D$, we shall have $ax = y = xa$.

Now $1y = 1(ax)$ [$\because ax = y$]

$= (1a)x = ax$ [$\because 1a = a$]

$= y$ [$\because ax = y$]

$= y1$ [$\because$ D is commutative]

Thus $1y = y = y1, \ \forall \ y \in D$. Therefore 1 is the unit element *i.e.*, the multiplicative identity of the ring D.

Now $1 \in D$. Therefore from the above discussion one of the n products $aa_1, aa_2, \ldots, aa_n$ will be equal to 1. Thus there exists an element, say, $b \in D$ such that $ab = 1 = ba$.

$\therefore$ b is the multiplicative inverse of the non-zero element $a \in D$. Thus every non-zero element of D is inversible.

Hence D is a field.

Illustrative Examples

Example 3: *If a, b, c are elements of a ring R , then evaluate* $(a + b)(c + d)$.

Solution: We have

$(a + b)(c + d) = a(c + d) + b(c + d)$ [by right distributive law]

$= ac + ad + bc + bd.$ [by left distributive law]

Example 4: *Prove that if* $a, b \in R$ *then* $(a + b)^2 = a^2 + ab + ba + b^2$, *where by* x^2 *we mean* $x\,x$.

Solution: We have $(a + b)^2 = (a + b)(a + b)$

$= a(a + b) + b(a + b)$ [by right distributive law]

$= (aa + ab) + (ba + bb)$ [by left distributive law]

$= a^2 + ab + ba + b^2.$

Example 5: *If* R *is a ring such that* $a^2 = a \;\forall\; a \in R$ *prove that*

(i) $a + a = 0 \;\forall\; a \in R$ *i.e., each element of* R *is its own additive inverse.* **(Kumaun 2008)**

(ii) $a + b = 0 \Rightarrow a = b.$ **(Kanpur 2005; Kumaun 08)**

(iii) R *is a commutative ring.* **(Meerut 2001)**

Solution: (i) $a \in R \Rightarrow a + a \in R.$

Now $(a + a)^2 = (a + a)$ [given]

$\Rightarrow$ $(a + a)(a + a) = a + a \Rightarrow (a + a)a + (a + a)a = a + a$ [Left Dist. Law]

$\Rightarrow$ $(a^2 + a^2) + (a^2 + a^2) = a + a$ [Right Dist. Law]

$\Rightarrow$ $(a + a) + (a + a) = a + a$ $[\because a^2 = a]$

$\Rightarrow$ $(a + a) + (a + a) = (a + a) + 0$ $[\because a + 0 = a]$

$\Rightarrow$ $(a + a) = 0$ [by left cancellation law for addition in R]

(ii) We have just proved that $a + a = 0$.

$\therefore$ $a + b = 0 \Rightarrow a + b = a + a \Rightarrow b = a,$

by left cancellation law for addition in R.

(iii) We have

$(a + b)^2 = (a + b) \Rightarrow (a + b)(a + b) = (a + b)$

$\Rightarrow$ $(a + b)a + (a + b)b = a + b$ [Left Dist. Law]

$\Rightarrow$ $(a^2 + ba) + (ab + b^2) = a + b$ [Right Dist. Law]

$\Rightarrow$ $(a + ba) + (ab + b) = a + b$ $[\because a^2 = a, b^2 = b]$

$\Rightarrow$ $(a + b) + (ba + ab) = (a + b) + 0$

[by commutativity and associativity of addition]

$\Rightarrow$ $ba + ab = 0$ [by left cancellation law for addition in R]

$\Rightarrow$ $ab = ba.$ [by part (ii) of this question]

$\therefore$ R is a commutative ring.

Note: An element a of a ring R is said to be idempotent if $a^2 = a$. *A ring R is called a* **Boolean Ring** *if all of its elements are idempotent i.e., if* $a^2 = a \quad \forall \quad a \in R$.

Example 6: *Prove that the set M of 2×2 matrices over the field of real numbers is a ring with respect to matrix addition and multiplication. Is it a commutative ring with unity element ? Find the zero element. Does this ring possess zero divisors ?*

Solution: Let $A, B \in M$. Then $A + B \in M$ and $AB \in M$. Therefore M is closed with respect to addition and multiplication of matrices.

Both addition and multiplication of matrices are associative compositions.

$\therefore \quad A + (B + C) = (A + B) + C \quad \forall \quad A, B, C \in M$

and $\quad A(BC) = (AB)C \quad \forall \quad A, B, C \in M.$

Addition of matrices is a commutative composition. Therefore for all $A, B \in M$, we have

$$A + B = B + A.$$

If O be the null matrix of the type 2×2, then

$$O \in M \text{ and } O + A = A \quad \forall \quad A \in M.$$

Further multiplication of matrices is distributive with respect to addition.

$\therefore \quad A(B + C) = AB + AC$

and $\quad (B + C)A = BA + CA \quad \forall \; A, B, C \in M.$

$\therefore$ M is a ring with respect to the given compositions.

Multiplication of matrices is not in general a commutative composition. For example, if $A = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, then

$$AB = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 3 & 11 \end{bmatrix}$$

and $$BA = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 8 & 14 \\ 3 & 5 \end{bmatrix}.$$

Thus $AB \neq BA$ and so the ring is a non-commutative ring.

If I be the unit matrix of the type 2×2 *i.e.*, if $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then $I \in M$. Also we have

$$AI = A = IA \quad \forall \quad A \in M.$$

$\therefore$ I is the multiplicative identity.

Thus the ring possesses the unit element and we have $I = 1$ (the unit element of the ring).

The null matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the additive identity and is therefore the zero element of the ring *i.e.*, $O = 0$ (the zero element of the ring).

The ring possesses zero divisors. For example if

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix},\ B = \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix},\ \text{then } AB = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring.

Example 7: *Show that the set of numbers of the form $a + b\sqrt{2}$, with a and b as rational numbers is a field.* **(Kumaun 2006, 07, 13, 14; Rohilkhand 08)**

Solution: Let $R = \{ a + b\sqrt{2} : a, b \in \mathbf{Q}\}$.

Let $a_1 + b_1\sqrt{2} \in R$ and $a_2 + b_2\sqrt{2} \in R$. Then $a_1, b_1, a_2, b_2 \in \mathbf{Q}$.

We have $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$

$\in R$ since $a_1 + a_2, b_1 + b_2 \in \mathbf{Q}$.

Also $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$

$\in R$ since $a_1a_2 + 2b_1b_2,\ a_1b_2 + a_2b_1 \in \mathbf{Q}$.

Thus R is **closed with respect to addition and multiplication**.

All the elements of R are real numbers and we know that addition and multiplication are both associative as well as commutative compositions in the set of real numbers.

Further we have $0 + 0\sqrt{2} \in R$ since $0 \in \mathbf{Q}$.

If $a + b\sqrt{2} \in R$, then

$(0 + 0\sqrt{2}) + (a + b\sqrt{2}) = (0 + a) + (0 + b)\sqrt{2} = a + b\sqrt{2}$.

$\therefore$ $0 + 0\sqrt{2}$ is the **additive identity**.

Again if $a + b\sqrt{2} \in R$, then $(-a) + (-b)\sqrt{2} \in R$ and we have

$[(-a) + (-b)\sqrt{2}] + (a + b\sqrt{2}) = 0 + 0\sqrt{2}$.

$\therefore$ each element of R possesses **additive inverse**.

Further in the set of real numbers **multiplication is distributive with respect to addition.**

Again $1 + 0\sqrt{2} \in R$ and we have

$(1 + 0\sqrt{2})(a + b\sqrt{2}) = (a + b\sqrt{2}) = (a + b\sqrt{2})(1 + 0\sqrt{2})$.

$\therefore$ $1 + 0\sqrt{2}$ is the **multiplicative identity**.

Thus R is a commutative ring with unity. The zero element of the ring is $0 + 0\sqrt{2}$ and the unit element is $1 + 0\sqrt{2}$.

Now R will be a field, if each non-zero element of R possesses multiplicative inverse.

Let $a + b\sqrt{2}$ be any non-zero element of this ring *i.e.*, at least one of a and b is not zero.

Then $$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

$$= \left(\frac{a}{a^2 - 2b^2}\right) + \left(-\frac{b}{a^2 - 2b^2}\right)\sqrt{2}\,.$$

Now if a and b are rational numbers, then we can have $a^2 = 2b^2$ only if $a = 0, b = 0$.

Since here at least one of the rational numbers a and b is not 0, therefore we cannot have $a^2 = 2b^2$ *i.e.*, $a^2 - 2b^2 = 0$.

$\therefore$ $\frac{a}{a^2 - 2b^2}$ and $-\frac{b}{a^2 - 2b^2}$ are both rational numbers and at least one of them is not zero.

$\therefore$ $\left(\frac{a}{a^2 - 2b^2}\right) + \left(-\frac{b}{a^2 - 2b^2}\right)\sqrt{2}$ is a non-zero element of R and is the multiplicative inverse of $a + b\sqrt{2}$.

Hence the given system is a field.

Example 8: ***A* Gaussian integer** *is a complex number $a + ib$, where a and b are integers. Show that the set $J[i]$ of Gaussian integers forms a ring under ordinary addition and multiplication of complex numbers. Is it an integral domain ? Is it a field ?*

Solution: Let $a + ib$ and $c + id$ be any two Gaussian integers.

Then $(a + ib) + (c + id) = (a + c) + i(b + d)$

and $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$.

These are again Gaussian integers. Therefore $J[i]$ is closed with respect to ordinary addition and multiplication of complex numbers.

Further in complex numbers both addition and multiplication are associative as well as commutative compositions. Also multiplication distributes with respect to addition. The Gaussian integer $0 + i\,0$ is the additive identity. The additive inverse of $a + ib$ is $(-a) + i(-b)$. The Gaussian integer $1 + i\,0$ is the multiplicative identity.

Therefore the set of Gaussian integers is a commutative ring with unity for the given compositions.

Also this ring is free from zero divisors since the product of two non-zero complex numbers cannot be zero. Therefore $J[i]$ is an integral domain.

But this is not a field since the multiplicative inverse of $a + ib$ will be

$$\frac{a}{a^2 + b^2} + i\left(-\frac{b}{a^2 + b^2}\right)$$

which is not always a Gaussian integer as $\frac{a}{a^2 + b^2}$ and $-\frac{b}{a^2 + b^2}$ are not necessarily integers.

Example 9: *Give an example of a skew field which is not a field.*

Solution: Let M be the set of all 2×2 matrices of the form

$$\begin{bmatrix} a + ib & c + id \\ -c + id & a - ib \end{bmatrix}, \text{ where } a, b, c, d \text{ are arbitrary real numbers.}$$

First we shall prove that M is a ring with respect to addition and multiplication of matrices.

Let $A = \begin{bmatrix} a + ib & c + id \\ -c + id & a - ib \end{bmatrix}$ and $B = \begin{bmatrix} p + iq & r + is \\ -r + is & p - iq \end{bmatrix}$ be any two elements of M.

We have

$$A + B = \begin{bmatrix} (a + p) + i(b + q) & (c + r) + i(d + s) \\ -(c + r) + i(d + s) & (a + p) - i(b + q) \end{bmatrix},$$

which is obviously a matrix of the given form. So

$$A + B \in M.$$

Also,

$$AB = \begin{bmatrix} (a + ib)(p + iq) & (a + ib)(r + is) \\ \quad + (c + id)(-r + is) & \quad + (c + id)(p - iq) \\ (-c + id)(p + iq) & (-c + id)(r + is) \\ \quad + (a - ib)(-r + is) & \quad + (a - ib)(p - iq) \end{bmatrix}$$

$$= \begin{bmatrix} (ap - bq - cr - ds) & (ar - bs + cp + dq) \\ \quad + i(aq + bp + cs - dr) & \quad + i(as + br - cq + dp) \\ -(cp + dq + ar - bs) & (-cr - ds + ap - bq) \\ \quad + i(dp - cq + as + br) & \quad - i(cs - dr + aq + bp) \end{bmatrix},$$

which is obviously an element of M. Thus M is closed with respect to addition and multiplication of matrices. Further matrix addition is commutative as well as associative. The zero matrix

$$\begin{bmatrix} 0 + i0 & 0 + i0 \\ -0 + i0 & 0 - i0 \end{bmatrix}$$

is the additive identity and so it is the zero element of M. If

$$A = \begin{bmatrix} a + ib & c + id \\ -c + id & a - ib \end{bmatrix} \in M,$$

then obviously

$$-A = \begin{bmatrix} -a - ib & -c - id \\ c - id & -a + ib \end{bmatrix} \in M.$$

Thus each element of M possesses additive inverse. Further matrix multiplication is associative and it is distributive with respect to addition. Hence M is a ring with respect to addition and multiplication of matrices.

Existence of multiplicative identity: The matrix

$$\begin{bmatrix} 1+i0 & 0+0\,i \\ -0+i0 & 1-i0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is obviously an element of M. It is the unit matrix and so it is the multiplicative identity. Thus M is a ring with unity.

Existence of multiplicative inverse of each non-zero element of M : Let

$$A = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$$

be any non-zero element of M *i.e.*, a, b, c, d are not all equal to zero. We have $|A|$ *i.e.*, $\det A = a^2 + b^2 + c^2 + d^2 \neq 0$. Therefore the matrix A is non-singular and is therefore inversible. We must show that $A^{-1} \in M$. Let $|A| = m$. Then m is a real number and $m > 0$. We have

$$A^{-1} = \frac{1}{|A|} \text{Adj. } A$$

$$= \frac{1}{m} \begin{bmatrix} a-ib & -c+id \\ c-id & a+ib \end{bmatrix},$$

which is obviously an element of M. Therefore each non-zero element of M possesses multiplicative inverse.

$\therefore$ M is a skew-field (or a division ring).

Now we shall show that M is not a field *i.e.*, multiplication in M is not commutative. We have

$$A = \begin{bmatrix} 3+4i & 5+6i \\ -5+6i & 3-4i \end{bmatrix} \in M,$$

and

$$B = \begin{bmatrix} 1+i0 & 1+i0 \\ -1+i0 & 1-i0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \in M.$$

Also

$$AB = \begin{bmatrix} -2-2\,i & 8+10\,i \\ -8+10\,i & -2+2\,i \end{bmatrix},$$

and

$$BA = \begin{bmatrix} -2+10\,i & 8+2\,i \\ -8+2\,i & -2-10\,i \end{bmatrix}.$$

We see that $AB \neq BA$. Therefore multiplication in M is not commutative and so M is not a field.

Hence M is a skew-field which is not a field.

Example 10: **Rings of Continuous Function:** *Show that the set R of all real valued continuous functions defined in the closed interval* $[0, 1]$ *is a commutative ring with unity with respect to the addition and multiplication of functions defined pointwise as follows :*

$$(f+g)(x) = f(x) + g(x)$$

and

$$(fg)(x) = f(x)\, g(x),$$

where f, g are any two members of R.

Solution: **Closure property:** If f is a real valued function in the closed interval $[0, 1]$, then we mean that $f(x)$ is a real number $\forall\ x \in [0, 1]$. We know that the sum and product of two real numbers are also real numbers. Also the sum and product of two continuous functions is also a continuous function. Therefore R is closed with respect to the given compositions.

Now let f, g, h be any three elements of R. Then we make the following observations.

Associativity of addition: For every $x \in [0, 1]$, we have

$$[(f + g) + h](x) = [(f + g)(x)] + h(x)$$
$$= [f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$$
$$[\because f(x),\ g(x), h(x) \text{ are real numbers and addition of real numbers is associative}]$$
$$= f(x) + (g + h)(x) = [f + (g + h)](x).$$
$$(f + g) + h = f + (g + h), \text{ by the equality of two mappings.}$$

Commutativity of addition: We have

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x)$$
$$[\because \text{addition of real numbers is commutative})$$
$$= (g + f)(x).$$
$$\therefore \quad f + g = g + f.$$

Existence of additive identity: Let us define a function e by the rule $e(x) = 0\ \ \forall\ \ x \in [0, 1]$. Then $e \in R$. Also if $f \in R$, we have

$$(e + f)(x) = e(x) + f(x) = 0 + f(x) = f(x).$$
$$\therefore \quad e + f = f$$

$\therefore$ the function e is the additive identity.

Existence of additive inverse: Let $f \in R$. Let us define a function $-f$ by the formula $(-f)(x) = -[f(x)]\ \forall\ x \in [0, 1]$.

Then $-f \in R$ and we have

$$[-f + f](x) = (-f)(x) + f(x) = -f(x) + f(x) = 0 = e(x).$$
$$\therefore \quad -f + f = e.$$

$\therefore$ the function $-f$ is the additive inverse of f.

Associativity of multiplication: We have

$$[(fg)h] = [(fg)(x)]h(x)$$
$$= [f(x)\, g(x)]h(x) = f(x)[g(x)h(x)]$$
$$= f(x)[(gh)(x)] = [f(gh)](x).$$
$$\therefore \quad (fg)h = f(gh).$$

Distributive laws: We have

$$[f(g+h)](x) = f(x)[(g+h)(x)] = f(x)[g(x)+h(x)]$$
$$= f(x)\,g(x) + f(x)\,h(x) = (fg)(x) + (fh)(x)$$
$$= [fg + fh](x).$$

$\therefore \quad f(g+h) = fg + fh$

Similarly we can prove that

$$(g+h)f = gf + hf.$$

$\therefore$ R is a ring with respect to the given compositions.

Commutativity of multiplication: We have

$$(fg)(x) = f(x)\,g(x) = g(x)\,f(x) = (gf)(x).$$

$\therefore \quad fg = gf.$

$\therefore$ R is a commutative ring.

Existence of multiplicative identity: Let us define a function i by the formula $i(x) = 1 \;\forall\; x \in [0, 1]$. Then $i \in R$. If $f \in R$. We have $(if)(x) = i(x)\,f(x) = 1\,f(x) = f(x)$.

$\therefore \quad if = f = fi$ [by commutativity of multiplication]

$\therefore$ The function i is the multiplicative identity.

Thus the ring R is with unity element.

The Ring of Integers Modulo p :

Example 11: *Let p be a prime number. Prove that the set of integers* $\mathbf{I}_p$,

$$\mathbf{I}_p = \{0, 1, 2, 3, \ldots\ldots, p-1\}$$

forms a field with respect to addition and multiplication modulo p.

Solution: As in the chapter on groups we can prove that $(\mathbf{I}_p, +_p)$ is an abelian group. Also $\mathbf{I}_p$ is closed with respect to '$\times_p$'. The composition '$\times_p$' is associative as well as commutative. Also '$\times_p$' is distributive with respect to '$+_p$' as can be proved as below :

Let $a, b, c \in \mathbf{I}_p$. Then

$$a \times_p (b +_p c) = a \times_p (b + c) \qquad [\because b +_p c \equiv b + c \pmod p]$$
$$= \text{least non-negative remainder when } a\,(b + c) \text{ is divided by } p$$
$$= \text{least non-negative remainder when } ab + ac \text{ is divided by } p$$
$$= (ab) +_p (ac)$$
$$= (a \times_p b) +_p (ac) \qquad [\because ab \equiv a \times_p b \pmod p]$$
$$= (a \times_p b) +_p (a \times_p c).$$

Similarly we can prove the other distributive law.

1 is the identity element for '$\times_p$'.

The zero element of the ring $(\mathbf{I}_p, +_p, \times_p)$ is 0. As in groups, we can prove that each non-zero element of $\mathbf{I}_p$ has multiplicative inverse.

In short the non-zero elements of $\mathbf{I}_p$ form an abelian group with respect to '$\times_p$'. Therefore $(\mathbf{I}_p, +_p, \times_p)$ is a field.

Note: If p is not prime, then this ring will have zero divisors and so it cannot be a field. Ring of residue classes modulo p is a field if and only if p is a prime.

Example 12: *Prove that the set of residue classes modulo p is a commutative ring with respect to addition and multiplication of residue classes. Further show that the ring of residue classes modulo p is a field if and only if p is a prime.* **(Bundelkhand 2007)**

Solution: Let $\mathbf{I}_p$ be the set of residue classes modulo p. Then $\mathbf{I}_p$ has p distinct elements. Thus $\mathbf{I}_p = \{ [0], [1], [2], \ldots, [p-1] \}$.

Let $[a], [b] \in \mathbf{I}_p$. Then we define addition and multiplication of residue classes as follows :

$$[a] + [b] = [a + b], \qquad \text{(Addition)}$$

$$[a]\,[b] = [ab]. \qquad \text{(Multiplication)}$$

Since $[a + b]$ and $[ab]$ are both residue classes modulo p, therefore $\mathbf{I}_p$ is closed with respect to addition and multiplication.

Now let $[a], [b], [c]$ be any elements of $\mathbf{I}_p$.

Then we observe :

Commutativity of Addition:

$$\begin{aligned} [a] + [b] &= [a + b] && \text{(by def. of addition of residue classes)} \\ &= [b + a] && (\because \text{ addition of integers is commutative}) \\ &= [b] + [a]. \end{aligned}$$

Associativity of Addition: We have

$$\begin{aligned} ([a] + [b]) + [c] &= [a + b] + [c] = [(a + b) + c] = [a + (b + c)] \\ &= [a] + [b + c] = [a] + ([b] + [c]). \end{aligned}$$

Existence of Additive Identity: We have $[0] \in \mathbf{I}_p$. If $[a] \in \mathbf{I}_p$,

then $[0] + [a] = [0 + a] = [a]$. Therefore $[0]$ is the additive identity.

Existence of Additive Inverse: Let $[a] \in \mathbf{I}_p$. Then $[-a] \in \mathbf{I}_p$.

We have

$$[-a] + [a] = [-a + a] = [0].$$

Therefore $[-a]$ is the additive inverse of $[a]$.

Associativity of Multiplication: We have

$$([a]\,[b])\,[c] = [ab]\,[c] = [(ab)\,c] = [a\,(bc)] = [a]\,[bc] = [a]\,([b]\,[c]).$$

Commutativity of Multiplication: We have $[a]\,[b] = [ab] = [ba] = [b]\,[a]$.

Distributive Laws: We have

$$[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac]$$
$$= [ab]+[ac] = [a][b]+[a][c].$$

Similarly $([b]+[c])[a] = [b][a]+[c][a]$.

Thus $\mathbf{I}_p$ is a commutative ring. Note that it is a finite ring because it has p elements. Now suppose that p is a prime number. Then to prove that $\mathbf{I}_p$ is a field. Let $[a], [b] \in \mathbf{I}_p$.

Then $[a][b] = [0]$

$\Rightarrow$ $[ab] = [0]$

$\Rightarrow$ p is a divisor of ab *i.e.*, $p \mid ab$

$\Rightarrow$ $p \mid a$ or $p \mid b$

[Note that if a and b are any two integers and p is a prime number, then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$]

$\Rightarrow$ $[a] = [0]$ or $[b] = [0]$.

Thus $\mathbf{I}_p$ is without zero divisors. Therefore $\mathbf{I}_p$ is an integral domain. But every finite integral domain is a field. Hence $\mathbf{I}_p$ is a field. Conversely suppose that $\mathbf{I}_p$ is a field. Then $\mathbf{I}_p$ is an integral domain. Therefore $\mathbf{I}_p$ is without zero divisors. We are to prove that p is a prime number. Suppose p is not prime, but p is composite. Let $p = mn$, where $1 < m < p$, $1 < n < p$. Then

$$[mn] = [p] \Rightarrow [m][n] = [0] \qquad (\because [p] = [0])$$

Also $[m] \neq [0]$, since $1 < m < p$. Similarly $[n] \neq 0$.

Thus $[m][n] = [0]$ while neither $[m] = [0]$ n or $[n] = [0]$.

Therefore $\mathbf{I}_p$ possesses zero divisors and thus we get a contradiction. Hence p must be prime.

Comprehensive Exercise 1

1. Prove that the set of rational numbers (real numbers or complex numbers) is a field with respect to addition and multiplication.
2. (i) Prove that the set of integers is an integral domain with respect to addition and multiplication.
 (ii) Define a field. Prove that every field is an integral domain, but there exist some integral domains which are not fields.
3. Define a ring and furnish an example of (i) a non-commutative ring with unity, (ii) a commutative ring without unity. **(Kumaun 2008, 10)**
4. (i) Prove that in the list of axioms for a ring R with unity the axiom demanding commutativity under addition may be omitted.

(ii) If R is a system satisfying all the conditions for a ring with unity with the possible exception $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.

(iii) Let $\boldsymbol{C}$ be the set of the ordered pairs (a, b) of real numbers. Define addition and multiplication in C by the equations

$(a, b) + (c, d) = (a + c, b + d)$, $(a, b)(c, d) = (ac - bd, bc + ad)$.

Prove that $\boldsymbol{C}$ is a field.

5. Is every field also a division ring ? Does the set of all integers under usual addition and multiplication form a field ? Give some example of a field which is finite.

6. Prove that the set of integers R, $R = \{0, 1, 2, 3, 4\}$ forms a field under addition modulo 5 and multiplication modulo 5. **(Kumaun 2008)**

7. (i) Prove that the set $\{0, 1, 2\} \pmod 3$ is a field with respect to addition and multiplication.

(ii) Prove that the ring $\mathbf{I}_3$ of integers modulo 3 is a field.

(iii) Prove that the set $\{0, 1\} \pmod 2$ is a field with respect to addition and multiplication.

8. (i) In a ring R prove that $-(-a) = a$. **(Meerut 2000)**

(ii) If two operations $*$ and o on the set $\mathbf{I}$ of integers are defined as follows : $a * b = a + b - 1, a \circ b = a + b - ab$,

prove that the system $(\mathbf{I}, *, \circ)$ is a commutative ring with identity.

(iii) If R is a ring with unity element 1, then $(-1)a = -a = a(-1)$ $\forall\, a \in R$ and $(-1)(-1) = 1$. **(Meerut 2000)**

9. Prove that the set of rational numbers with two operations $*$ and o defined by $a * b = a + b - 1, a \circ b = a + b - ab$ is a field. **(Meerut 2000)**

10. If addition and multiplication modulo 10 is defined on the set of integers $R = \{0, 2, 4, 6, 8\}$, prove that the resulting system is a ring with unity. Is it an integral domain ?

11. Do the following sets form integral domains with respect to ordinary addition and multiplication ? If so, state if they are fields.

(i) The set of numbers of the form $b\sqrt{2}$ with b rational.

(ii) The set of even integers.

(iii) The set of positive integers.

12. If a ring R has a left identity as well as right identity, then prove that the two are equal.

13. Prove that the only idempotent elements of an integral domain with unity are 0 and 1.

14. An element a of a ring R is said to be **nilpotent** if $a^n = 0$ for some positive integer n. Prove that $a = 0$ is the only nilpotent element of an integral domain.

15. (i) If R is a commutative ring, prove by induction that

$$(a+b)^n = a^n + {}^nc_1\ a^{n-1}\ b + {}^nc_2\ a^{n-2}\ b^2 + \ldots + b^n$$

for every positive integer n; here a and b are elements of R.

(ii) Prove that a ring R is commutative if and only if

$(a+b)^2 = a^2 + 2ab + b^2 \quad \forall\ a, b \in R$. **(Gorakhpur 2012; Kumaun 12)**

16. Explain with examples the difference between a field, a skew-field and an integral domain.

17. Give an example each of :

(i) a commutative ring without unity.

(ii) a non-commutative ring.

(iii) a ring without zero divisors.

(iv) division ring.

18. If in a ring with unity any element a has the multiplicative inverse, then a cannot be a divisor of zero.

19. If a, b, c, d are elements of a ring R, prove that

(i) $a - b = c - d \Leftrightarrow a + d = b + c$.

(ii) $(a-b)(c-d) = (ac + bd) - (ad + bc)$. **(Kumaun 2007)**

20. Prove that in a field

(i) $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc$.

(ii) $\dfrac{a}{b} - \dfrac{c}{d} = \dfrac{ad - bc}{bd}$.

(iii) $(-a)^{-1} = -(a^{-1})$.

(iv) $\dfrac{(-a)}{(-b)} = \dfrac{a}{b}$.

21. (i) Show that $Z[\sqrt{(-5)}]$, the set of complex numbers $a + b\sqrt{(-5)}$ where a, b are integers, is an integral domain.

(ii) Prove that the set $\mathbf{I}(\sqrt{2})$ of numbers of the form $a + b\sqrt{2}$, with a and b as integers is an integral domain with respect to ordinary addition and multiplication. Is it a field ? **(Kumaun 2008)**

22. (i) Prove that the totality R of all ordered pairs (a, b) of real numbers is a commutative ring with zero divisors under the addition and multiplication of ordered pairs defined as

$(a, b) + (c, d) = (a + c, b + d),\ (a, b)(c, d) = (ac, bd) \quad \forall\ (a, b), (c, d) \in R$.

(ii) Define a ring and an integral domain. Give an example of a ring which is not an integral domain.

23. (i) Show that the set of all matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$, a and b being real numbers, is a ring with matrix addition and matrix multiplication as the two ring compositions. Is it a commutative ring? **(Gorakhpur 2014)**

(ii) Show that the set R of all real valued continuous functions defined in the closed interval [0, 1] is a commutative ring with unity with respect to the addition and multiplication of functions defined pointwise as follows :

$(f + g)(x) = f(x) + g(x)$ *and* $(fg)(x) = f(x)\, g(x)$,

where f, g are any two members of R.

Answers 1

5. Yes; No; $(\{0, 1, 2\}, +_3, \times_3)$ is a finite field.

10. Yes

11. (i) No

(ii) Yes, provided we do not require the existence of unity element for an integral domain. But it is not a field.

(iii) No

21. (ii) No

23. No

9 Characteristic of a Ring

Definition: *Let R be a ring with zero element* 0 *and suppose there exists a positive integer n such that* $na = a + a + \ldots$ *upto n terms* $= 0$ *for every* $a \in R$. *The smallest such positive integer n is called the characteristic of the ring. If there exists no such positive integer, then R is said to be of characteristic zero or infinite.* **(Gorakhpur 2011)**

Illustration 1: If any element of a ring R is of order zero when regarded as an element of the additive group $(R, +)$, then R will be of zero characteristic.

Illustration 2: The ring of integers is of characteristic zero. The ring of rational numbers is also of characteristic zero.

Illustration 3: If $\mathbf{I}_6 = \{0, 1, 2, 3, 4, 5\}$, then the ring $(\mathbf{I}_6, +_6, \times_6)$ *i.e.*, the ring of integers modulo 6 has characteristic 6 since $6x = 0$ for every x in the ring. Obviously, no integer smaller than 6 satisfies this property. For instance, 5 cannot be the characteristic, since $5(2) = 4$ in $\mathbf{I}_6$ and $4 \neq 0$.

Theorem 1: *The characteristic of a ring with unity is* 0 *or* $n > 0$ *according as the unity element* 1 *regarded as a member of the additive group of the ring has the order zero or* n.

Proof: Let R be a ring with unity element 1. If 1 has order zero, then the characteristic of the ring is zero.

Suppose 1 is of finite order n so that

$$1 + 1 + 1 + \ldots \text{ upto } n \text{ terms} = 0 \text{ } i.e., \text{ } n1 = 0.$$

Let a be any element of R. Then, we have

$$\begin{aligned} na &= a + a + \ldots \text{ upto } n \text{ terms} \\ &= 1a + 1a + 1a + \ldots \text{ upto } n \text{ terms} \\ &= (1 + 1 + 1 + \ldots \text{ upto } n \text{ terms})\, a \qquad \text{[by dist. law]} \\ &= (n1)\, a = 0a = 0. \end{aligned}$$

$\therefore$ order of a is $\leq n$.

Hence the characteristic of the ring is n.

Theorem 2: *The characteristic of an integral domain is* 0 *or* $n > 0$ *according as the order of any non-zero element regarded as a member of the additive group of the integral domain is either* 0 *or* n. **(Gorakhpur 2010, 13; Kumaun 13)**

Proof: Let D be an integral domain.

If a non-zero element a of D is of order zero, then the characteristic of D is zero.

Let the order of the non-zero element a be finite and equal to n. Then $na = 0$.

Suppose b is any other non-zero element of D.

We have $na = 0$

$$\Rightarrow \quad (na)\, b = 0$$

$$\Rightarrow \quad (a + a + a + \ldots \text{ upto } n \text{ terms})\, b = 0$$

$$\Rightarrow \quad (ab + ab + ab + \ldots \text{ upto } n \text{ terms}) = 0$$

$$\Rightarrow \quad a\,(b + b + b + \ldots \text{ upto } n \text{ terms}) = 0$$

$$\Rightarrow \quad a\,(nb) = 0.$$

But D is without zero divisors. Therefore $a \neq 0$ and $a\,(nb) = 0 \Rightarrow nb = 0$.

But the order of a is $n \Rightarrow n$ is the least positive integer such that $na = 0$. Also we have $n0 = 0$. Thus n is the least positive integer such that $nx = 0\ \forall\ x \in D$. Hence D is of characteristic n.

Theorem 3: *Each non-zero element of an integral domain D, regarded as a member of the additive group of D, is of the same order.*

Proof: Let D be an integral domain. Suppose a is a non-zero element of D and $o(a)$ is finite and say, equal to n.

Suppose b is any other non-zero element of D and $o(b) = m$.

We have $o(a) = n \Rightarrow na = 0$

$\Rightarrow$ $nb = 0$ [See Theorem 2]

$\Rightarrow$ $o(b) \leq n \Rightarrow m \leq n$.

Similarly,

$o(b) = m \Rightarrow mb = 0 \Rightarrow a(mb) = 0$

$\Rightarrow$ $a(b + b + \ldots$ upto m times$) = 0$

$\Rightarrow$ $(ab + ab + ab + \ldots$ upto m times$) = 0$

$\Rightarrow$ $(a + a + a + \ldots$ upto m times$)\, b = 0$

$\Rightarrow$ $(ma)\, b = 0$

$\Rightarrow$ $ma = 0$ [$\because b \neq 0$ and D is without zero divisors]

$\Rightarrow$ $o(a) \leq m \Rightarrow n \leq m$.

Now $m \leq n, n \leq m \Rightarrow m = n$.

Hence $o(a) = o(b)$.

Also if $o(a)$ is zero, then $o(b)$ cannot be finite. Because $o(b) = m \Rightarrow ma = 0$ *i.e.*, the order of a is finite. Hence $o(b)$ must also be zero. Hence the theorem.

10 Characteristic of an Integral Domain

(Kumaun 2006, 14)

Theorem : *The characteristic of an integral domain is either* 0 *or a prime number.*

Proof: Suppose D is an integral domain. Let $0 \neq a \in D$. If $o(a)$ is zero, then the characteristic of D is 0. If $o(a)$ is finite, let $o(a) = p$. Then the characteristic of D will be p. We are to prove that p must be prime.

Suppose p is not prime. Let $p = p_1\ p_2$ where $p_1 \neq 1, p_2 \neq 1$ and $p_1 < p$ also $p_2 < p$.

Since D is an integral domain, therefore the product of two non-zero elements of D cannot be equal to 0.

$\therefore$ $aa \neq 0$ *i.e.*, $a^2 \neq 0$.

Now in an integral domain two non-zero elements are of the same order.

$\therefore$ $o(a) = p \Rightarrow o(a^2) = p$

$\Rightarrow$ $pa^2 = 0$

$\Rightarrow$ $(p_1\ p_2)\, a^2 = 0$ [$\because p = p_1\ p_2$]

$\Rightarrow$ $(a^2 + a^2 + a^2 + \ldots$ upto $p_1\ p_2$ terms$) = 0$

$\Rightarrow$ $(p_1\ a)\,(p_2\ a) = 0$

$\Rightarrow$ either $p_1\ a = 0$ or $p_2\ a = 0$. [$\because D$ is without zero divisors]

But $p_1 < p$ and $p_2 < p$. Also p is the least positive integer such that $pa = 0$. Hence p must be prime.

11 Characteristic of a Field

Every field is an integral domain. Therefore the characteristic of a field F is 0 or $n > 0$ according as any non-zero element (in particular the unit element 1) of F is of order 0 or n.

Thus in order to find the characteristic of field F, we should find the order of the unit element 1 of F when regarded as a member of the additive group of F. If the order of 1 is zero, then F is of characteristic 0. If the order of 1 is finite, say, n then the characteristic of F is n.

Illustration 1: The characteristic of the field of real numbers is 0.

Illustration 2: The characteristic of the finite field $(\mathbf{I}_7, +_7, \times_7)$ is 7,

where $\mathbf{I}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

12 Ordered Integral Domains

Definition: *An integral domain $(D, +, .)$ is said to be ordered if D contains a subset D_+ such that*

(i) D_+ is closed with respect to addition and multiplication as defined on D.

(ii) $\forall$ $a \in D$, one and only one of $a = 0$, $a \in D_+$, $-a \in D_+$ holds.

(Principle of Trichotomy)

The elements of D_+ are called the *positive* elements of D, all other non-zero elements of D are called *negative* elements of D.

13 Ordered Field

A field $(F, +, .)$ is said to be ordered if it is ordered as an integral domain.

Illustration 1: The integral domain $(\mathbf{I}_+, +, .)$ of all integers is ordered.

Illustration 2: The set $\mathbf{I}_+$ of all positive integers is the set of the positive elements of this integral domain. We know that the sum and product of two positive integers is again a positive integer *i.e.*, $\mathbf{I}_+$ is closed with respect to addition and multiplication. If $a \in \mathbf{I}$, then either a is zero or positive or negative *i.e.*, either $a = 0$ or $a \in \mathbf{I}_+$ or $-a \in \mathbf{I}_+$.

Illustration 3: The field of rational numbers is an ordered field. The field of real numbers is also an ordered field. But the field of complex numbers is not an ordered field.

Theorem 1: *Let D be an integral domain with unity element* 1. *If D is an ordered integral domain show that* 1 *is a positive element of D.*

Proof: Let D be an ordered integral domain with unity element 1. Let D_+ denote the set of positive elements of D.

Suppose $1 \notin D_+$.

Now $1 \neq 0$. Since $1 \notin D_+$, therefore by the definition of an ordered integral domain,

$-1 \in D_+$

$\Rightarrow$ $(-1)(-1) \in D_+$ [$\because D_+$ is closed with respect to multiplication]

$\Rightarrow$ $1 \in D_+$ which is a contradiction.

Hence $1 \in D_+$ *i.e.,* 1 is a positive element of D.

Theorem 2: *The field* $(\mathbf{C}, +, .)$ *of complex numbers is not ordered.*

Proof: Suppose $\mathbf{C}$ is an ordered field and $\mathbf{C}_+$ is the set of positive elements of this field. The additive identity *i.e.,* the zero element is $0 + i0$.

Now $i \neq 0$.

By the principle of trichotomy either $i \in \mathbf{C}_+$ or $-i \in \mathbf{C}_+$.

Now $\mathbf{C}_+$ is closed with respect to multiplication.

$\therefore$ $i \in \mathbf{C}_+, -1 \in \mathbf{C}_+ \Rightarrow i(-1) = -i \in \mathbf{C}_+$. Thus if $i \in \mathbf{C}_+$, its additive inverse $-i$ also belongs to $\mathbf{C}_+$. This contradicts the principle of trichotomy *i.e.,* the condition (ii) of the definition of an ordered integral domain.

Similarly if we assume that $-i \in \mathbf{C}_+$, we can show that its additive inverse i also belongs to $\mathbf{C}_+$. This again contradicts the principle of trichotomy.

Hence the field of complex numbers is not an ordered field.

14 Order Relations in an Ordered Integral Domain

Definition: *Let D be an ordered integral domain and D_+ be the set of positive elements of D. Then we define 'less than'* $(<)$ *, 'greater than'* $(>)$ *relations in D as follows:*

For all $a, b \in D$, we have

(i) $a > b$ *when* $a - b \in D_+$,

(ii) $a < b$ *when* $b - a \in D_+$.

Obviously $a > b$ iff $b < a$.

Theorem: *The order relation in an ordered integral domain is transitive i.e.,*

$a > b, b > c \Rightarrow a > c$.

Proof: Let D be an ordered integral domain and let D_+ be the set of positive elements of D.

We have $a > b \Rightarrow a - b \in D_+$ [by def. of >]

and $b > c \Rightarrow b - c \in D_+$.

Now D_+ is closed with respect to addition.

$\therefore$ $a - b \in D_+, b - c \in D_+ \Rightarrow (a - b) + (b - c) \in D_+$

$\Rightarrow$ $a - c \in D_+ \Rightarrow a > c$.

Comprehensive Exercise 2

1. Let x, y be commutative elements of a ring R of characteristic two. Show that $(x + y)^2 = x^2 + y^2 = (x - y)^2$.
2. Let R be a non-zero ring such that for all $a \in R, a^2 = a$. Prove that R is a commutative ring of characteristic 2.
3. Show that every finite integral domain is of finite characteristic.
4. Show that in an integral domain all non-zero elements generate additive cyclic groups of the same order which is equal to the characteristic of the integral domain.
5. Give without proof, an example of an integral domain which contains only five elements. Is this an ordered integral domain ? Give reason.
6. Define the characteristic of a ring and prove that if R is a finite ring then the characteristic of R is finite and $\neq 0$.
7. Define an ordered field and illustrate the concept with the help of an example.

Objective Type Questions

Multiple Choice Questions

Indicate the correct answer for each question by writing the corresponding letter from (a), (b), (c) *and* (d).

1. The algebraic structure $(\{0, 1, 2, 3\}, +_4, \times_4)$ is

 (a) a ring (b) an integral domain

 (c) a field (d) a skew field

2. The ring of 2×2 matrices with elements as integers is a ring with unity. Its unity element is the matrix

(a) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

(c) $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ (d) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

3. In the ring $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$, the additive inverse of 2 is

(a) 1 (b) 4

(c) 3 (d) 2 **(Kumaun 2009)**

4. In the ring of 2×2 matrices over the field of real numbers, the zero element of the ring is the matrix

(a) $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (d) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

5. The field of rational numbers is of characteristic

(a) 0 (b) 1

(c) 2 (d) none of these

6. If $(R, +, \bullet)$ is a ring with unity element and $a, b, c \in R$, then which of the following statement is false ?

(a) $a \bullet (b - c) = a \bullet b + a \bullet c$ (b) $a \bullet 0 = 0 \bullet a = 0$

(c) $(-a) \bullet (-b) = a \bullet b$ (d) $1 \bullet (-1) = -1$

(Kumaun 2006, 07, 11)

7. The characteristics of the field $(I_7, +_7, \times_7)$ is

(a) 8 (b) 7

(c) 6 (d) 4 **(Kumaun 2006)**

8. Which of the following algebraic structures is not field ?

(a) $(R, +, \bullet)$ (b) $(Z, +, \bullet)$

(c) $(Q, +, \bullet)$ (d) $(C, +, \bullet)$

(Kumaun 2007, 11, 13)

9. Which one is correct ?

The ring of integers $(Z, +, \bullet)$ is

(a) a skew field (b) a field

(c) a boolean ring (d) an integral domain

(Kumaun 2008, 13, 14, 15)

10. A commutative ring R with unity elements is called a field if
(a) it is with proper zero divisors
(b) every non zero element in it has a multiplicative inverse
(c) it is without proper zero divisor
(d) none of these **(Kumaun 2008, 15)**

11. Every division ring is a field, if it is
(a) associative (b) commutative
(c) distributive (d) none of these **(Kumaun 2010)**

12. In the field $(\{0,1,2,3,4\}, +_5, \times_5)$ the multiplicative inverse of 4 is
(a) 3 (b) 1
(c) 2 (d) 4 **(Kumaun 2010, 14)**

Fill in the Blank(s)

Fill in the blanks "……", so that the following statements are complete and correct.

1. If the algebraic structure $(R, +, \bullet)$ is a ring, then the algebraic structure $(R, +)$ is an …… .

2. The element of a ring which is identity for the addition of the ring is called the …… of the ring.

3. A ring R is said to be a commutative ring if $ab = \ldots\ldots$, $\forall\ a, b \in R$.

4. A ring R is said to be a ring with unity if it possesses multiplicative …… .

5. If R is a ring, then $a0 = \ldots\ldots$, $\forall\ a \in R$.

6. If R is a ring then $(-a)(-b) = \ldots\ldots$, $\forall\ a, b \in R$.

7. A ring R is said to be a ring without zero divisors if the product of no two non-zero elements of R is …… .

8. In the field of rational numbers, the multiplicative inverse of $-3/7$ is …… .

9. In the field $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$,
(i) the multiplicative inverse of 3 is …… and
(ii) the additive inverse of 1 is …… .

10. In the field of complex numbers the multiplicative inverse of $3 + 4i$ is $\frac{3}{25}$ where $b = \ldots\ldots$.

11. The non-zero elements of a field form an …… with respect to multiplication.

12. If p is a positive integer greater than 1, then the ring $(\{0, 1, 2, \ldots\ldots, p-1\}, +_p, \times_p)$ is a field if and only if p is …… .

13. Every finite integral domain is always a …… .

14. The only elements of the ring of integers which possess multiplicative inverse are …… .

15. In a ring R , $-(-a) = \ldots\ldots$, $\forall \ a \in R$.

16. If a is any non-zero element of a field F, then $(a^{-1})^{-1} = \ldots\ldots$.

True or False

Write 'T' for true and 'F' for false statement.

1. Every integral domain is a field.

2. A field can possess zero divisors.

3. Every field is an integral domain.

4. Every finite integral domain is a field.

5. A ring R is a commutative ring if $a + b = b + a$, $\forall \ a, b \in R$.

6. If a and b are any two elements of a ring R, then $(a + b)^2 = a^2 + 2ab + b^2$.

7. If a and b are any two elements of a commutative ring R, then $(a + b)^2 = a^2 + 2ab + b^2$.

8. The ring of even integers is a ring with unity.

9. The ring of complex numbers is also a field.

10. The ring of integers is also an integral domain.

11. The ring $(\{0, 1, 2, 3, 4, 5\}, +_6 , \times_6)$ possesses zero divisors.

12. The ring $(\{0, 1, 2\}, +_3 , \times_3)$ possesses zero divisors.

13. The ring $(\{ 0, 1, 2, 3, 4\}, +_5 , \times_5)$ is a field. **(Meerut 2003)**

14. The ring of integers is a ring without zero divisors.

15. The ring of 2×2 matrices with elements as integers is a non-commutative ring.

16. The ring of 2×2 matrices with elements as real numbers is a ring without zero divisors.

17. In a ring R , if $ab = 0$, then we must have $ba = 0$.

18. In any ring R if $a, b, c \in R$ and $a \neq 0$, then $ab = ac \Rightarrow b = c$.

19. If R is a ring without zero divisors and $a, b, c \in R$ and $a \neq 0$, then $ab = ac \Rightarrow b = c$.

20. In a field F , if $ab = 0$, then we must have $ba = 0$.

21. The characteristic of the ring of integers is 1.

22. There can exist a field whose characteristic is 4.

23. The characteristic of the field $(\{0, 1, 2\}, +_3 , \times_3)$ is 3.

24. The characteristic of the field of rational numbers is 2.

Answers

Multiple Choice Questions

1.	(a)	**2.**	(b)	**3.**	(c)	**4.**	(d)	**5.**	(a)
6.	(a)	**7.**	(b)	**8.**	(b)	**9.**	(a)	**10.**	(b)
11.	(b)	**12.**	(b)						

Fill in the Blank(s)

1. abelian group
2. zero element
3. *ba*
4. identity
5. 0
6. *ab*
7. zero
8. $-\frac{7}{3}$
9. (i) 2 (ii) 4
10. $\frac{4}{25}$
11. abelian group
12. prime
13. field
14. 1 and –1
15. *a*
16. *a*

True or False

1.	*F*	**2.**	*F*	**3.**	*T*	**4.**	*T*	**5.**	*F*
6.	*F*	**7.**	*T*	**8.**	*F*	**9.**	*T*	**10.**	*T*
11.	*T*	**12.**	*F*	**13.**	*T*	**14.**	*T*	**15.**	*T*
16.	*F*	**17.**	*F*	**18.**	*F*	**19.**	*T*	**20.**	*T*
21.	*F*	**22.**	*F*	**23.**	*T*	**24.**	*F*		

□

Chapter

2

Subrings and Ideals

1 Subrings

Definition: *Let R be a ring. A non-empty subset S of the set R is said to be a subring of R if S is closed with respect to the operations of addition and multiplication in R and S itself is a ring for these operations.* **(Meerut 2001; Kumaun 10, 12; Gorakhpur 13)**

If S is a subring of a ring R, it is obvious that S is a subgroup of the additive group of R.

Improper and Proper Subrings: If R is any ring, then $\{0\}$ and R itself are always subrings of R. These are known as **improper subrings** of R. Other subrings, if any, of R are called **proper subrings** of R.

Illustration 1: The set of all $n \times n$ matrices over the field of rational numbers is a subring of the ring of all $n \times n$ matrices over the field of real numbers.

Conditions for a Subring:

Theorem: *The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are*

(i) $a \in S, b \in S \Rightarrow a - b \in S$ (ii) $a \in S, b \in S \Rightarrow ab \in S$.

(Gorakhpur 2015)

Proof: The conditions are necessary: Suppose $(S, +, .)$ is a subring of $(R, +, .)$.

Since S is a group with respect to addition, therefore $b \in S \Rightarrow -b \in S$.

Now S is closed with respect to addition.

$\therefore \quad a \in S, b \in S \Rightarrow a \in S, -b \in S \Rightarrow a + (-b) \in S \Rightarrow a - b \in S.$

Also S is closed with respect to multiplication.

$\therefore \quad a \in S, b \in S \Rightarrow ab \in S.$

Hence the conditions are necessary.

The conditions are sufficient: Suppose S is a non-empty subset of R and the conditions (i) and (ii) are satisfied. From (i), we have

$a \in S, a \in S \Rightarrow a - a \in S \Rightarrow 0 \in S$ *i.e.*, the zero element $\in S$.

Now since $0 \in S$, therefore from (i), we have

$0 \in S, a \in S \Rightarrow 0 - a \in S \Rightarrow -a \in S$ *i.e.*, each element of S possesses additive inverse.

Now if a, b are any elements of S, then $-b \in S$.

From (i), we have

$a \in S, -b \in S \Rightarrow a - (-b) \in S \Rightarrow a + b \in S.$

$\therefore$ S is closed with respect to addition.

Now S is a subset of R. Therefore associativity and commutativity of addition must hold in S since they hold in R.

$\therefore$ $(S, +)$ is an abelian group.

From (ii) S is closed with respect to multiplication.

Associativity of multiplication and distributivity of multiplication over addition must hold in S since they hold in R.

Hence S is a subring of R.

Corollary: *The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are*

(i) $S + (-S) = S$ (ii) $SS \subseteq S$.

Proof: The conditions are necessary: Suppose S is a subring of R. Then S is a subgroup of the additive group of R.

Let $a + (-b)$ be any element of $S + (-S)$.

We have $a + (-b) \in S + (-S) \Rightarrow a \in S, -b \in -S \Rightarrow a \in S, b \in S$

$\Rightarrow \quad a - b \in S$ [$\because$ S is a subgroup]

$\therefore \quad S + (-S) \subseteq S.$

Also let a be any element of S. We can write $a = a + 0$.

Now S is a subgroup. Therefore $0 \in S$ or $0 \in -S$.

So $a + 0 \in S + (-S)$. $\therefore \quad S \subseteq S + (-S)$.

$\therefore \quad S = S + (-S)$.

Also S must be closed with respect to multiplication.

$\therefore \quad a \in S, b \in S \Rightarrow ab \in S$.

Now ab is an arbitrary element of SS.

$\therefore \quad SS \subseteq S$.

The conditions are sufficient: Suppose S is a non-empty subset of R satisfying the two given conditions.

We have $SS \subseteq S \Rightarrow ab \in S \; \forall \; a, b \in S$.

Therefore S is closed with respect to multiplication.

Also $S + (-S) = S \Rightarrow S + (-S) \subseteq S$.

$\Rightarrow \quad a + (-b) \in S$ if $a, b \in S$

$\Rightarrow \quad S$ is a subgroup of the additive group of R.

$\therefore \quad S$ is a subring of R.

Intersection of Subrings :

Theorem 1: *The intersection of two subrings is a subring.*
(Meerut 2000, 12, 13; Kumaun 06, 07, 10, 14; Avadh 13; Gorakhpur 11, 14)

Proof : Let S_1 and S_2 be two subrings of a ring R. Then $S_1 \cap S_2$ is not empty since at least $0 \in S_1 \cap S_2$.

Now in order to prove that $S_1 \cap S_2$ is a subring, it is sufficient to prove that

(i) $a \in S_1 \cap S_2 \; , b \in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$

(ii) $a \in S_1 \cap S_2 \; , b \in S_1 \cap S_2 \Rightarrow ab \in S_1 \cap S_2$.

We have $a \in S_1 \cap S_2 \Rightarrow a \in S_1, a \in S_2$,

$b \in S_1 \cap S_2 \Rightarrow b \in S_1, b \in S_2$.

Now S_1 and S_2 are both subrings.

$\therefore \quad a \in S_1, b \in S_1 \Rightarrow a - b \in S_1$ and $ab \in S_1$

and $a \in S_2 \; , b \in S_2 \Rightarrow a - b \in S_2$ and $ab \in S_2$.

Now $a - b \in S_1, a - b \in S_2 \Rightarrow a - b \in S_1 \cap S_2$

and $ab \in S_1, ab \in S_2 \Rightarrow ab \in S_1 \cap S_2$.

Thus $a \in S_1 \cap S_2 \; , b \in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$.

$\therefore \; S_1 \cap S_2$ is a subring of R.

Theorem 2: *An arbitrary intersection of subrings is a subring.*

Proof: Let R be a ring and let $\{ S_t : t \in T \}$ be any family of subrings of R. Here T is an index set and is such that $\forall \; t \in T$, S_t is a subring of R. Let

$$S = \bigcap_{t \in T} S_t = \{x \in R : x \in S_t \; \forall \; t \in T \}$$

be the intersection of this family of subrings of R. Then to prove that S is also a subring of R .

Obviously $S \neq \emptyset$, since at least the zero element 0 of R is in $S_t \ \forall \ t \in T$.

Now let a, b be any two elements of S. Then

$$a \in \bigcap_{t \in T} S_t \Rightarrow a \in S_t \ \forall \ t \in T$$

and $$b \in \bigcap_{t \in T} S_t \Rightarrow b \in S_t \ \forall \ t \in T.$$

But $\forall \ t \in T, S_t$ is a subring of R. Therefore,

$$a, b \in S_t \Rightarrow a - b, ab \in S_t \ \forall \ t \in T.$$

Consequently,

$$a - b, ab \in \bigcap_{t \in T} S_t.$$

Thus we have shown that

$$a, b \in \bigcap_{t \in T} S_t \Rightarrow a - b, ab \in \bigcap_{t \in T} S_t.$$

Therefore $\bigcap_{t \in T} S_t$ is a subring of R.

Illustrative Examples

Example 1: *The set of integers is a subring of the ring of rational numbers.*

Solution : If $a, b \in \mathbf{I}$, then $a - b \in \mathbf{I}$ and $ab \in \mathbf{I}$.

$\therefore$ $\mathbf{I}$ is a subring of the ring of rational numbers.

Example 2: *Let R be the ring of all 2×2 matrices over the field of real numbers. Let M be a subset of R and let the elements of M be matrices of the type* $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$

i.e., matrices in which the elements of second column are all zeros. Then M is a subring of R.

Solution: Let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ be any two elements of M.

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix}$. Also $AB = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ b_1 a_2 & 0 \end{bmatrix}$.

Now $A - B$ and AB are both members of M since the second column of $A - B$ and also of AB consists of zeros only.

$\therefore$ M is a subring of R.

Example 3: *Show that the set of matrices* $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ *is a subring of the ring of 2×2 matrices with integral elements.* **(Gorakhpur 2013)**

Solution: Let R be the ring of 2×2 matrices and let M be the subset of R and let the elements of M be matrices of the type $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$.

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ be any two elements of M.

Then $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix}$ which is obviously an element of M.

Also $AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix}$

which is obviously an element of M.

$\therefore$ M is a subring of R.

Example 4: *Let R be the ring of integers. Let m be any fixed integer and let S be any subset of R such that*

$S = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$. *Then S is a subring of R.*

Solution: Let $a = rm$ and $b = sm$ be any two elements of S. Then r and s are some integers. We have

$$a - b = rm - sm = (r - s)\, m \quad \text{and} \quad ab = (rm)\,(sm) = (rsm)\, m.$$

Since $r - s$ is some integer and (rsm) is also some integer, therefore both $a - b$ and ab are elements of S. Hence S is a subring of R.

2 Subfields

Definition: *Let F be a field. A non-empty subset K of the set F is said to be a subfield of F if K is closed with respect to the operations of addition and multiplication in F and K itself is a field for these operations.*

Conditions for a Subfield:

Theorem: *The necessary and sufficient conditions for a non-empty subset K of a field F to be a subfield of F are*

(i) $a \in K,\ b \in K \Rightarrow a - b \in K$, (ii) $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$.

(Meerut 2000, 12, 12B; Gorakhpur 15)

Proof: The conditions are necessary: Suppose K is a subfield of the field F. Now K is a group with respect to addition. Therefore $b \in K \Rightarrow -b \in K$. Also K is closed with respect to addition.

$\therefore$ $a \in K, b \in K \Rightarrow a + (-b) \in K \Rightarrow a - b \in K$.

Now each non-zero element of K possesses multiplicative inverse. Therefore

$$0 \neq b \in K \Rightarrow b^{-1} \in K.$$

But K is closed with respect to multiplication.

$\therefore$ $a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K$.

Hence the conditions are necessary.

The conditions are sufficient: Suppose K is a non-empty subset of F and the conditions (i) and (ii) are satisfied.

As we have proved in subrings, we can prove that with the help of condition (i), $(K, +)$ is an abelian group. [Give the same proof here].

Now let a be any non-zero element of K.

Then from (ii), we have

$$a \in K, 0 \neq a \in K \Rightarrow aa^{-1} \in K \Rightarrow 1 \in K.$$

Now $1 \in K$, therefore again from (ii), we have

$$1 \in K, 0 \neq a \in K \Rightarrow 1a^{-1} \in K \Rightarrow a^{-1} \in K.$$

$\therefore$ Each non-zero element of K possesses multiplicative inverse.

Now let $a \in K$ and $0 \neq b \in K$. Then $b^{-1} \in K$.

From (ii), we have

$$a \in K, 0 \neq b^{-1} \in K \Rightarrow a\,(b^{-1})^{-1} \in K \Rightarrow ab \in K.$$

Also if $b = 0$, then $ab = 0$ and $0 \in K$.

$\therefore$ $ab \in K \ \forall \ a, b \in K$.

Associativity of multiplication and distributivity of multiplication over addition must hold in K since they hold in F.

Hence K is a subfield of F.

Illustration: The field of real numbers is a subfield of the field of complex numbers. The field of rational numbers is a subfield of the field of real numbers.

Comprehensive Exercise 1

1. Show that the set of all 2-rowed matrices of the form $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ where a, b, c are integers is a subring of the ring M of all 2-rowed matrices with integral entries.
2. Give an example to show that the union of two subrings is not necessarily a subring.

3. Prove or disprove that any subring of a non-commutative ring is non-commutative.
4. Show that the set of even integers forms a subring of the ring of integers.
5. If R is a ring, show that $Z(R) = \{x \in R : xy = yx \ \forall \ y \in R\}$ is a subring of R. Further show that $Z(R)$ is a field if R is a division ring.

3 Ideals

(a) Left Ideal:

A non-empty subset S of a ring R is said to be a left ideal of R if :

(*i*) *S is a subgroup of R with respect to addition.*

(*ii*) $rs \in S \ \forall \ r \in R$ *and* $\forall \ s \in S$.

(b) Right Ideal:

A non-empty subset S of a ring R is said to be a right ideal of R if :

(*i*) *S is a subgroup of R under addition,*

(*ii*) $sr \in S \ \forall \ r \in R$ *and* $\forall \ s \in S$.

(c) Ideal: **(Kumaun 2009, 11)**

A non-empty subset S of a ring R is said to be an *ideal* (also *a two sided ideal*) if and only if it is both a left ideal and a right ideal. *Thus a non-empty subset S of a ring R is said to be an ideal of R if :*

(*i*) *S is a subgroup of R under addition i.e., S is a subgroup of the additive group of R.*

(*ii*) $rs \in S$ *and* $sr \in S$ *for every* $r \in R$ *and for every* $s \in S$. **(Gorakhpur 2015)**

If S is an ideal of a ring R, then S is also a subring of R. The obvious reason is that S is a subgroup of R under addition and from condition (ii), we have $xs \in S \ \forall \ x, s \in S$ because $x \in S \Rightarrow x \in R$. Thus S is closed with respect to multiplication. Therefore S is a subring of R. *Thus every ideal of a ring R is also a subring of R*. But every subring is not an ideal. An ideal requires a stronger closure property than the subring. If S is a subgroup of R under addition, then S will be a subring if S is closed with respect to multiplication *i.e.*, the product of two elements of S is again in S. But S will be an ideal if the product of any element of S with any element of R is in S.

If R is a commutative ring, then every left ideal will also be a right ideal. Therefore in a commutative ring every left (right) ideal is an ideal.

Note 1: If we are to prove that a non-empty subset S of a ring R is an ideal of R, then it is sufficient to prove that

(i) $a \in S, b \in S \Rightarrow a - b \in S$

(ii) $rs \in S$ and $sr \in S \ \forall \ r \in R$ and $\forall \ s \in S$.

Obviously (i) is a sufficient condition for S to be a subgroup of R under addition.

If R is a commutative ring, then the condition (ii) will become more simple. Then it will become

$$rs \in S \ \forall \ \ r \in R \text{ and } \forall \ \ s \in S.$$

Note 2: Every ring R always possesses two **improper ideals** : one R itself and the other consisting of 0 only. These are respectively known as the **unit ideal** and the **null ideal**.

Any other ideals of R are called **proper ideals.** A ring having no proper ideals is called **a simple ring**. **(Kumaun 2006, 11)**

4 Algebra of Ideals

Theorem 1: *The intersection of any two left ideals of a ring is again a left ideal of the ring.* **(Kumaun 2007, 10, 15)**

Proof: Let I_1 and I_2 be two left ideals of a ring R. Then I_1, I_2 are subgroups of R under addition. Therefore $I_1 \cap I_2$ is also a subgroup of R under addition.

Now to show that $I_1 \cap I_2$ is a left ideal of R, we are only to show that $r \in R$,

$$s \in I_1 \cap I_2 \Rightarrow rs \in I_1 \cap I_2.$$

We have $s \in I_1 \cap I_2 \Rightarrow s \in I_1, s \in I_2$.

But I_1 and I_2 are left ideals of R. Therefore

$$r \in R, s \in I_1 \Rightarrow rs \in I_1 \text{ and } r \in R, s \in I_2 \Rightarrow rs \in I_2.$$

Now $rs \in I_1, rs \in I_2 \Rightarrow rs \in I_1 \cap I_2$.

$\therefore$ $I_1 \cap I_2$ is also a left ideal of R.

Note: A similar result can be proved for right ideals as well as for ideals.

Theorem 2: *An arbitrary intersection of left ideals of a ring is a left ideal of the ring.*

Proof: Let R be a ring and let $\{S_t : t \in T\}$ be any family of left ideals of R. Here T is an index set and is such that $\forall \ \ t \in T, S_t$ is a left ideal of R. Let

$$S = \bigcap_{t \in T} S_t = \{ x \in R : x \in S_t \ \forall \ \ t \in T \}$$

be the intersection of this family of left ideals of R. Then to prove that S is also a left ideal of R.

Obviously $S \neq \varnothing$, since at least 0 is in $S_t \ \ \forall \ \ t \in T$.

Now let a, b be any two elements of S. Then

$$a, b \in S \Rightarrow a, b \in S_t \ \forall \ \ t \in T$$

$\Rightarrow$ $a - b \in S_t \ \ \forall \ \ t \in T$ $\quad [\because \ \forall \ t \in T, S_t \text{ is a left ideal of } R]$

$\Rightarrow$ $a - b \in \bigcap_{t \in T} S_t \Rightarrow a - b \in S.$

Now let a be any element of S and r be any element of R.

We have $a \in S \Rightarrow a \in \underset{t \in T}{\cap} S_t \ \forall \ t \in T$

$\Rightarrow$ $r\,a \in S_t \ \forall \ t \in T$ [$\because \forall\, t \in T, S_t$ is a left ideal of R]

$\Rightarrow$ $r\,a \ \underset{t \in T}{\cap} S_t \Rightarrow ra \in S$.

Thus $a, b \in S \Rightarrow a - b \in S$ and $r \in R, a \in S \Rightarrow ra \in S$.

$\therefore$ S is a left ideal of R.

5 Smallest Left Ideal containing a given Subset

Definition: *Let M be a non-empty subset of a ring. Then a left ideal I of R is called the smallest left ideal of R containing M, if I contains M and if I is contained in every left ideal of R containing M.*

The smallest left ideal of R containing M is called the **left ideal generated by** M and will be denoted by (M).

Note: A similar definition can be given for the right ideal generated by M as well as for the ideal generated by M. For this purpose simply replace the word 'left ideal' by 'right ideal' or by 'ideal'.

6 Sum of Two Left Ideals

Theorem 1: *The left ideal generated by the union $I_1 \cup I_2$ of the left ideals is the set $I_1 + I_2$ consisting of the elements of R obtained on adding any element of I_1 to any element of I_2 .*

Proof: Let $a_1 + a_2 \ , b_1 + b_2 \in I_1 + I_2$.

Then $a_1 , b_1 \in I_1$ and $a_2 , b_2 \in I_2$.

Since I_1 , I_2 are left ideals of R, therefore they are subgroups of the additive group of R. Therefore,

$$a_1 , b_1 \in I_1 \Rightarrow a_1 - b_1 \in I_1 \text{ and } a_2 , b_2 \in I_2 \Rightarrow a_2 - b_2 \in I_2 .$$

Consequently,

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I_1 + I_2 .$$

Therefore $I_1 + I_2$ is a subgroup of the additive group of R.

Now let $r \in R$ and $a_1 + a_2 \in I_1 + I_2$. Then $a_1 \in I_1 , a_2 \in I_2$.

We have $r\,(a_1 + a_2) = ra_1 + ra_2 \in I_1 + I_2 .$

[$\because I_1$ is a left ideal implies $ra_1 \in I_1$ and similarly $ra_2 \in I_2$]

$\therefore$ $I_1 + I_2$ is a left ideal of R.

Since $0 \in I_2$, therefore $a_1 \in I_1$ can be written as $a_1 + 0$. Thus

$a_1 \in I_1 \Rightarrow a_1 \in I_1 + I_2$.

$\therefore \quad I_1 \subseteq I_1 + I_2$.

Similarly $\quad I_2 \subseteq I_1 + I_2$.

$\therefore \quad I_1 \cup I_2 \subseteq I_1 + I_2$.

Thus $I_1 + I_2$ is a left ideal containing $I_1 \cup I_2$.

Also if any left ideal contains $I_1 \cup I_2$, then it must contain $I_1 + I_2$.

$\therefore \quad I_1 + I_2$ is the smallest left ideal containing $I_1 \cup I_2$.

$\therefore \quad I_1 + I_2 =$ the left ideal generated by $I_1 \cup I_2 = (I_1 \cup I_2)$.

Note: A similar result can be proved for right ideals as well as for ideals.

Theorem 2: *Let S_1, S_2 be ideals of a ring R and let*

$$S_1 + S_2 = \{s_1 + s_2 : s_1 \in S_1, s_2 \in S_2\}.$$

Then $S_1 + S_2$ is an ideal of R generated by $S_1 \cup S_2$.

Proof: Let $a_1 + a_2 \in S_1 + S_2$, $b_1 + b_2 \in S_1 + S_2$. Then

$$a_1, b_1 \in S_1 \text{ and } a_2, b_2 \in S_2.$$

We have

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2).$$

Since S_1 is an ideal, therefore

$$a_1, b_1 \in S_1 \Rightarrow a_1 - b_1 \in S_1 .$$

Similarly $\quad a_2 - b_2 \in S_2$.

$\therefore \quad (a_1 - b_1) + (a_2 - b_2) \in S_1 + S_2$.

$\therefore \quad (a_1 + a_2) - (b_1 + b_2) \in S_1 + S_2$.

$\therefore \quad S_1 + S_2$ is a subgroup of the additive group of R.

Let r be any element of R. Then

$$r(a_1 + a_2) = r a_1 + r a_2 \in S_1 + S_2$$

since $r \in R, a_1 \in S_1 \Rightarrow ra_1 \in S_1$ and similarly $r a_2 \in S_2$.

Similarly,

$$(a_1 + a_2) r = a_1 r + a_2 r \in S_1 + S_2 \text{ since } a_1 r \in S_1, a_2 r \in S_2.$$

Hence $S_1 + S_2$ is an ideal of R.

Since $0 \in S_1$ and also $0 \in S_2$, therefore obviously

$$S_1 \subseteq S_1 + S_2 \text{ and } S_2 \subseteq S_1 + S_2.$$

$\therefore \quad S_1 \cup S_2 \subseteq S_1 + S_2$.

Thus $S_1 + S_2$ is an ideal of R containing $S_1 \cup S_2$.

Also if S is any ideal of R containing $S_1 \cup S_2$, then S must contain $S_1 + S_2$.

Thus $S_1 + S_2$ is the smallest ideal of R containing $S_1 \cup S_2$ *i.e.*,

$$S_1 + S_2 = (S_1 \cup S_2).$$

Illustrative Examples

Example 5: *The set N of all* 2×2 *matrices of the form* $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ *for a, b integers is a left ideal but not a right ideal in the ring R of all* 2×2 *matrices with elements as integers. Here N is the subset of R consisting of those elements whose second column contains only zeros.*

Solution: Let $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$ be any two elements of N.

Then $$A - B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in N.$$

$\therefore$ N is a subgroup of R under addition.

Now let $U = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of R and $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ be any element of N.

Then $$U\,A = \begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} wa + xb & 0 \\ ya + zb & 0 \end{bmatrix} \in N.$$

Therefore N is a left ideal of R. It is not a right ideal, since

$$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in N, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \in R,$$

and the product $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$ which is not an element of N.

Example 6: *If m is a fixed integer, the set P of integers given by*

$$P = \{ x\,m : x \text{ is an integer} \}$$

is an ideal of the ring R of all integers.

Solution: Let $x_1\ m$ and $x_2\ m$ be any two elements of P. Then x_1 and x_2 are some integers.

We have $x_1\ m - x_2\ m = (x_1 - x_2)\ m \in P$ since $x_1 - x_2$ is also an integer.

$\therefore$ P is a subgroup of R under addition.

Now let r be any integer *i.e.*, r be any element of R and xm be any element of P. Then $r\ (xm) = (r\ x)\ m \in P$ since $r\ x$ is also an integer. Therefore P is a left ideal of R. But R is a commutative ring. Hence P is an ideal of R.

Example 7: *The set of integers is only a subring but not an ideal of the ring of rational numbers* $(\mathbf{Q}, +, .)$.

Solution: The product of a rational number and an integer is not necessarily an integer.

For example $3 \in \mathbf{I}, 2/5 \in \mathbf{Q}$ but $(2/5).3 = 6/5 \notin \mathbf{I}$.

$\therefore$ **I** is not an ideal of the ring of rational numbers.

Example 8: *The set* **Q** *of rational numbers is only a subring but not an ideal of the ring of real numbers* $(\mathbf{R}, +, .)$.

Solution: The product of a rational number and a real number is not necessarily a rational number. For example $\frac{1}{2} \in \mathbf{Q}, \sqrt{7} \in \mathbf{R}$ but $\frac{1}{2} \cdot \sqrt{7} = \frac{\sqrt{7}}{2} \notin \mathbf{Q}$.

$\therefore$ **Q** is not an ideal of the ring of real numbers.

Example 9: *Prove that the subset S of all matrices of the form* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ *with a and b integers, forms a subring of the ring of all* 2×2 *matrices having elements as integers. Prove further that S is neither a right ideal nor a left ideal in R.*

Solution: Let $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$ be any two elements of S. Then

$$A - B = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S.$$

Also $$AB = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S.$$

$\therefore$ S is a subring of R.

Further $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S, \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \in R$ and the product

$$\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \notin S.$$

Therefore S is not a left ideal.

Again $$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 1 \end{bmatrix} \notin S.$$

Therefore S is not a right ideal.

Example 10: *If U is an ideal of a ring R with unity and* $1 \in U$ *prove that* $U = R$.

(Gorakhpur 2013)

Solution: We have $U \subseteq R$ since U is an ideal of R. Let x be any element of R. Since U is an ideal of R, therefore

$$1 \in U, x \in R \Rightarrow 1x \in U \Rightarrow x \in U.$$

$\therefore$ $R \subseteq U$.

$\therefore$ $U = R$.

Example 11: *If R is a ring and $a \in R$ and let $T = \{x \in R : a\,x = 0\}$, prove that T is a right ideal of R.*

Solution: First we see that U is not empty because

$0 \in R$ is such that $a0 = 0$.

Let x_1, x_2 be any two elements of T. Then $a\,x_1 = 0, a\,x_2 = 0$.

We have $a\,(x_1 - x_2) = a\,x_1 - a\,x_2 = 0 - 0 = 0$.

$\therefore$ $x_1 - x_2 \in T$.

$\therefore$ T is a subgroup of R under addition.

Now to show that T is a right ideal of R we are to show that $x \in T, y \in R \Rightarrow xy \in T$.

But $x \in T \Rightarrow ax = 0$. If we show that $a\,(xy) = 0$, then xy will be an element of T.

We have $a\,(xy) = (ax)\,y = 0\,y = 0$.

$\therefore$ $xy \in T$.

$\therefore$ T is a right ideal of R.

Example 12: *Prove that the intersection of two ideals of a ring R is an ideal of R.*

(Avadh 2012; Meerut 12, 13B; Kumaun 09, 13)

Solution: Let S and T be two ideals of a ring R. Then S, T are subgroups of R under addition. Therefore $S \cap T$ is also a subgroup of R under addition.

Now to show that $S \cap T$ is an ideal of R, we are only to show that

$r \in R, s \in S \cap T \Rightarrow rs \in S \cap T, sr \in S \cap T$.

We have $s \in S \cap T \Rightarrow s \in S, s \in T$.

But S and T are ideals of R. Therefore

$r \in R, s \in S \Rightarrow rs \in S, sr \in S$ and $r \in R, s \in T \Rightarrow rs \in T, sr \in T$.

Now $rs \in S, rs \in T \Rightarrow rs \in S \cap T$ and $sr \in S, sr \in T \Rightarrow sr \in S \cap T$.

$\therefore$ $S \cap T$ is also an ideal of R.

Example 13: *For any given element a of a ring R let $Ra = \{xa : x \in R\}$. Prove that Ra is a left ideal of R.*

Solution: Let $x_1\,a, x_2\,a$ be any two elements of Ra where $x_1, x_2 \in R$.

We have $x_1\,a - x_2\,a = (x_1 - x_2)\,a \in Ra$, since

$x_1, x_2 \in R \Rightarrow x_1 - x_2 \in R$.

Thus $x_1\,a, x_2\,a \in Ra \Rightarrow x_1\,a - x_2\,a \in Ra$.

Now let xa be any element of Ra where $x \in R$ and r be any element of R.

We have $r\,(xa) = (r\,x)\,a \in Ra$, since

$r \in R, x \in R \Rightarrow r\,x \in R$.

Thus $r \in R, xa \in Ra \Rightarrow r\,(xa) \in Ra$.

$\therefore$ Ra is a left ideal of R.

Example 14: *If U is an ideal of a ring R, let*

$$[R : U] = \{x \in R : r\,x \in U \ \forall\ r \in R\}.$$

Prove that $[R : U]$ is an ideal of R and that it contains U.

Solution: First we see that $[R : U]$ is not empty because $0 \in R$ is such that $r\,0 = 0 \in U$ for all $r \in R$.

Now let x_1, x_2 be any two elements of $[R : U]$. Then

$$r\,x_1 \in U \ \forall\ r \in R, \text{ and } r\,x_2 \in U \ \forall\ r \in R.$$

Since U is an ideal, therefore

$$r\,x_1 \in U, r\,x_2 \in U \ \Rightarrow\ r\,x_1 - r\,x_2 \in U$$

$$\Rightarrow \quad r\,(x_1 - x_2) \in U \ \forall\ r \in R$$

$$\Rightarrow \quad x_1 - x_2 \in [R : U], \text{ by def. of } [R : U].$$

Now let x be any element of $[R : U]$ and s be any element of R.

Then $\quad r\,x \in U \ \forall\ r \in R$

$$\Rightarrow \quad (r\,x)\,s \in U \ \forall\ r \in R$$

$$[\because\ U \text{ is an ideal and so } s \in R, r\,x \in U \Rightarrow (r\,x)\,s \in U]$$

$$\Rightarrow \quad r\,(xs) \in U \text{ for all } r \in R \Rightarrow\ xs \in [R : U].$$

Also $\quad r\,x \in U \ \forall\ r \in R \Rightarrow\ sx \in U \qquad [\because s \in R]$

$$\Rightarrow \quad (sx)\,r \in U \ \forall\ r \in R$$

$$[\because\ U \text{ is an ideal and so } sx \in U,\ r \in R \Rightarrow (sx)\,r \in U]$$

$$\Rightarrow \quad sx \in [R : U].$$

Thus $\quad x \in [R : U], s \in R \Rightarrow\ xs \in [R : U], sx \in [R : U].$

Therefore $[R : U]$ is an ideal of R.

Now to show that $U \subseteq [R : U]$. We have

$$y \in U \Rightarrow\ yr \in U \ \forall\ r \in R \qquad [\because\ U \text{ is an ideal}]$$

$$\Rightarrow \quad y \in [R : U].$$

$$\therefore \quad U \subseteq [R : U].$$

Comprehensive Exercise 2

1. Distinguish between Subrings and Ideals in a ring. Show that the 2-rowed matrices of the form $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ where a, b, c are integers form a subring of the ring of all 2-rowed matrices with integral entries. Is this subring an integral domain ?

2. Show that the set M of all 2×2 matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$

a, b integers is a left ideal but not a right ideal in the ring of all 2×2 matrices with elements as integers.

3. Show that for a field F, the set of all matrices of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$

for $a, b \in F$ is a right ideal but not a left ideal of the ring of all 2×2 matrices over the field F.

4. Show that S is an ideal of $S + T$ where S is any ideal of ring R and T any subring of R.

5. If U is a left ideal of a ring R, let

$$\lambda(U) = \{x \in R : xu = 0 \ \forall \ u \in U\}.$$

Prove that $\lambda(U)$ is a two sided ideal of R.

6. If U, V are ideals of a ring R, let UV be the set of all those elements of R which can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R . Also show that $UV \subseteq U \cap V$.

7. If U, V are ideals of a ring R, let $U + V = \{u + v : u \in U, v \in V\}$.

Prove that $U+V$ is also an ideal of R.

8. Show that an arbitrary intersection of ideals of a ring is an ideal of the ring.

9. If U is an ideal of a ring R, let $r(U) = \{x \in R : xu = 0 \ \forall \ u \in U\}$. Prove that $r(U)$ is an ideal of R.

10. Consider the ring R of all 3×3 matrices of the type $\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}$,

a, b, c, d, e, f are real numbers. Show that the set **I** of all matrices of the form $\begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, is a left ideal of R, which is not a right ideal.

11. Verify the following for being true or false :

(i) The set of all positive rationals is a subring of the ring of all rational numbers.

(ii) A subring of any field is a field.

(iii) Any subring of the ring of integers, Z, is an ideal of Z.

Answers 2

1. No

11. (i) false (ii) false (iii) true

7 More about Ideals

Theorem 1: *A field has no proper ideals i.e., if F is a field then its only ideals are* (0) *and F itself.* **(Kumaun 2009; Gorakhpur 13, 15)**

Proof: Let S be any non-zero ideal of the field F and let a be any non-zero element of S. We have $a^{-1} \in F$.

Since S is an ideal, therefore

$$a \in S, a^{-1} \in F \Rightarrow aa^{-1} \in S \Rightarrow 1 \in S.$$

Now let x be any element of F. Then

$$1 \in S, x \in F \Rightarrow 1x \in S \Rightarrow x \in S.$$

Thus each element of F belongs to S. Therefore $F \subseteq S$. But $S \subseteq F$. Therefore $S = F$. Thus the only ideals of F are (0) and F itself.

Theorem 2: *If R is a commutative ring and* $a \in R$, *then*

$$Ra = \{r\ a : r \in R\} \text{ is an ideal of } R.$$

(Kumaun 2009, 13; Gorakhpur 12)

Proof: In order to prove that Ra is an ideal of R, we should prove that Ra is a subgroup of R under addition and that if $u \in Ra$ and $x \in R$ then xu and ux are also in Ra. But R is a commutative ring, therefore $xu = ux$. Thus we only need to check that xu is in Ra.

Now, let $u, v \in Ra$. Then $u = r_1\ a, v = r_2\ a$ for some $r_1, r_2 \in R$.

We have $u - v = r_1\ a - r_2\ a = (r_1 - r_2)\ a \in Ra$ since $r_1 - r_2 \in R$.

Thus $u, v \in Ra \Rightarrow u - v \in Ra$. Hence Ra is a subgroup of R under addition.

Now let $x \in R$.

Then $xu = x\ (r_1\ a) = (x\ r_1)\ a \in Ra$ since $x\ r_1 \in R$.

$\therefore$ Ra is an ideal of R.

Theorem 3: *A commutative ring with unity is a field if it has no proper ideals.* **(Meerut 2013B)**

Proof: Let R be a commutative ring with unity having no proper ideals *i.e.*, the only ideals of R are (0) and R itself. In order to show that R is a field, we should show that each non-zero element of R possesses multiplicative inverse.

Let a be any non-zero element of R.

The set $Ra = \{ra : r \in R\}$ is an ideal of R. [See Theorem 2]

Since $1 \in R$, therefore $1a = a \in Ra$. Thus $0 \neq a \in Ra$. Therefore the ideal $Ra \neq (0)$. Since R has no proper ideals, therefore the only possibility is that $Ra = R$. Thus every element of R is a multiple of a by some element of R. In particular, $1 \in R$ so it can be realized as a multiple of a. Thus there exists an element $b \in R$ such that $ba = 1$. Therefore $a^{-1} = b$. Hence each non-zero element of R possesses multiplicative inverse.

$\therefore$ R is a field.

Note: *A commutative ring R with identity is a field if and only if it has no proper ideals.*

8 Ideal Generated by a given Subset of a Ring

If M is any subset of a ring R, we can find ideals containing M. For example, the ring R itself is an ideal containing any subset of R.

Smallest ideal containing a subset: Let M be any arbitrary subset of a ring R. Then an ideal S of R is called the *smallest ideal of R containing M if* $M \subseteq S$, and if S is contained in every ideal of R containing M.

Definition: *Let R be a ring and let M be any arbitrary subset of R. The smallest ideal of R containing M is said to be the ideal generated by M and is denoted by* (M).

In particular, if M consists of single element, say a, of the ring R we write (a) in place of (M). An ideal such as (a) generated by a single element of the ring is called a *principal ideal.*

Principal Ideal: Definition: *An ideal S of a ring R is said to be a principal ideal if there exists an element* $a \in S$ *such that an ideal T of R containing a also contains S i.e.,* $S = (a)$.

Thus an ideal generated by a single element of itself is called a principal ideal.
If a ring R has a unity element 1, then the ideal generated by 1 is the whole ring *i.e.*, $(1) = R$, since every element $r \in R$ may be written as $r\ 1$. For this reason ring itself is called the **unit ideal**. The ideal generated by the zero element of R *i.e.*, (0) consists of the zero element alone and is called the **null ideal**. Every ring R has at least one principal ideal, namely, (0). Every ring with unity has at least two principal ideals, namely, (0) and (1).

Theorem 1: *If a is an element in a commutative ring R with unity, then the set* $S = \{r\ a : r \in R\}$ *is a principal ideal of R generated by the element a i.e.,* $S = (a)$.

Proof: First we should prove that $a \in S$. Since R is a ring with unit element 1, therefore $1\ a = a \in S$.

Now we should prove that S is an ideal of R. So first we should prove that S is a subgroup of R under addition. Let u, v be any two elements of S. Then $u = r_1\ a$, $v = r_2\ a$ for some $r_1, r_2 \in R$.
We have $u - v = r_1\ a - r_2\ a = (r_1 - r_2)\ a \in S$ since $r_1 - r_2 \in R$.
$\therefore$ S is a subgroup of R under addition.
Now we should prove that $x \in R,\ u \in S \Rightarrow x\ u \in S$ and $ux \in S$. But R is a commutative ring, therefore $x\ u = u\ x$ and thus it is sufficient to show that $x\ u \in S$.
We have $x\ u = x\ (r_1\ a) = (x\ r_1)\ a \in S$ since $xr_1 \in R$.
$\therefore$ S is an ideal of R and $a \in S$.
Now in order to prove that S is an ideal generated by the element a, we should prove that if T is an ideal of R and $a \in T$, then $S \subseteq T$.
Let ra be any element of S. Then $r \in R$. If T is an ideal of R containing a, then $a \in T, r \in R \Rightarrow ra \in T$. Thus $S \subseteq T$.
Hence S is a principal ideal of R generated by the element a.

Illustration: *Suppose we are to find the principal ideal generated by* 5 *in the ring of integers.* The ring **I** of integers is a commutative ring with unity. Therefore $(5) = \{5r : r \in \mathbf{I}\}$.

Thus the principal ideal generated by 5 is given by

$$(5) = \{\ldots, -10, -5, 0, 5, 10, \ldots\}.$$

Obviously $(-5) = (5)$.

Theorem 2: *Let S be an ideal of a commutative ring R. Let a be an element of S such that*

$$x \in S \Rightarrow x = ya \text{ for some } y \in R.$$

Then S is a principal ideal of R generated by a.

Proof: As given in the statement of the theorem, S is an ideal of R containing the element a. Let T be any ideal of R containing a. Then S will be a principal ideal of R generated by a if $S \subseteq T$.

Let x be any element of S. Then $x = y\,a$ for some $y \in R$.

Now $\quad y \in R, a \in T \Rightarrow y\,a \in T \quad [\because T \text{ is an ideal}]$

$\Rightarrow \quad x \in T. \quad [\because x = y\,a]$

Thus $\quad x \in S \Rightarrow x \in T.$

$\therefore \quad S \subseteq T.$

Hence S is a principal ideal of R generated by a.

Note: The above theorem will be very helpful in proving that an ideal S of a commutative ring R is a principal ideal. If we are able to find an element a in S such that

$$x \in S \Rightarrow x = ay \text{ for some } y \in R,$$

then S will be a principal ideal of R generated by a.

9 Principal Ideal Ring

Definition: *A commutative ring R without zero divisors and with unity element is a principal ideal ring if every ideal S in R is a principal ideal i.e., if every ideal S in R is of the form $S = (a)$ for some $a \in S$.*

Theorem 1: *The ring of integers is a principal ideal ring.*

(Gorakhpur 2011, 12; Meerut 13B)

Proof: Let $(\mathbf{I}, +, .)$ be the ring of integers. Obviously **I** is a commutative ring with unity and without zero divisors. Therefore **I** will be a principal ideal ring if every ideal in **I** is a principal ideal.

Let S be any ideal of the ring of integers. If S is the null ideal then $S = (0)$ so that S is a principal ideal.

So let us suppose that $S \neq (0)$.

Now S contains at least one non-zero integer, say a. Since S is a subgroup of R under addition, therefore $a \in S \Rightarrow -a \in S$. This shows that S contains at least one positive integer, because if $0 \neq a$, then one of a and $-a$ must be positive.

Let S_+ be the set of all positive integers in S. Since S_+ is not empty, therefore by the well ordering principal S_+ must possess a least positive integer. Let s be this least element. We will now show that S is the principal ideal generated by s *i.e.*, $S = (s)$.

Suppose now that n is any integer in S. Then by division algorithm, there exist integers q and r such that $n = qs + r$ with $0 \le r < s$.

Now $s \in S, q \in \mathbf{I} \Rightarrow qs \in S$ [$\because S$ is an ideal]

and $n \in S, qs \in S \Rightarrow n - qs \in S$

[$\because S$ is a subgroup of the additive group of $\mathbf{I}$]

$\Rightarrow$ $r \in S$. [$\because n - qs = r$]

But $0 \le r < s$ and s is the least positive integer such that $s \in S$. Hence r must be 0.

$\therefore$ $n = qs$.

Thus $n \in S \Rightarrow n = qs$ for some $q \in \mathbf{I}$.

Hence S is a principal ideal of $\mathbf{I}$ generated by s.

Since S was an arbitrary ideal in the ring of integers, therefore the ring of integers is a principal ideal ring.

Theorem 2: *Every field is a principal ideal ring.*

Proof: A field has no proper ideals. The only ideals of a field are (i) the null ideal which is a principal ideal generated by 0 and (ii) the field itself which is also a principal ideal generated by 1. Thus a field is always a principal ideal ring.

10 Quotient Rings or Rings of Residue Classes

Suppose R is an arbitrary ring and S is an ideal (two sided ideal) in R. Then S is a subgroup of the additive abelian group of R. We can form the cosets (right as well as left) of S in R. Since R is an abelian additive group, therefore if $a \in R$, then the right coset $S + a$ will be equal to the corresponding left coset $a + S$. Thus we shall call $S + a$ as simply a coset of S in R. We remember from our study of cosets in group theory, that if $a, b \in R$, then $S + a = S + b \Leftrightarrow a - b \in S$.

The cosets of S in R are called the residue classes of S in R. We denote the set of all residue classes of S in R by the symbol R / S.

Thus $R / S = \{S + a : a \in R\}$.

We shall now impose a ring structure on the set R / S by defining addition and multiplication of residue classes.

Theorem: *If S is an ideal of a ring R, then the set $R / S = \{S + a : a \in R\}$ of all residue classes of S in R forms a ring for the two compositions in R / S defined as follows :*

$(S + a) + (S + b) = S + (a + b)$ [*Addition of residue classes*]

$(S + a)(S + b) = S + ab$ [*Multiplication of residue classes*]

(Gorakhpur 2014)

Proof: Since $S + (a + b)$ and $S + ab$ are also residue classes of S in R, therefore R / S is closed with respect to addition and multiplication of residue classes. First of all, we shall show that both addition and multiplication in R / S are well defined. For this we are to show that if $S + a = S + a'$ and $S + b = S + b'$, then

$$(S + a) + (S + b) = (S + a') + (S + b')$$

and $\quad (S + a)\,(S + b) = (S + a')\,(S + b')$.

We have $\quad S + a = S + a' \Rightarrow a' \in S + a$

and $\quad S + b = S + b' \Rightarrow b' \in S + b$.

Therefore there exist $\alpha, \beta \in S$ such that $a' = \alpha + a,\ b' = \beta + b$.

Now $\quad a' + b' = (\alpha + a) + (\beta + b) = (a + b) + (\alpha + \beta)$.

$\therefore \quad (a' + b') - (a + b) = \alpha + \beta \in S$.

$\therefore \quad S + (a' + b') = S + (a + b)$

$\Rightarrow \quad (S + a') + (S + b') = (S + a) + (S + b)$.

Thus addition in R / S is well defined.

Again $\quad a'\,b' = (\alpha + a)(\beta + b) = \alpha\beta + \alpha b + a\beta + ab$

$$= ab + \alpha\beta + \alpha b + a\beta.$$

$\therefore \quad a'\,b' - ab = \alpha\beta + \alpha b + a\beta \in S$.

[Since S is an ideal therefore $\alpha, \beta \in S$ and $a, b \in R \Rightarrow \alpha b \in S,\ a\beta \in S, \alpha\beta \in S$ and finally $\alpha\beta + \alpha b + a\beta \in S$].

Now since $a'\,b' - ab \in S$, therefore $S + a'\,b' = S + ab$

$\Rightarrow \quad (S + a')\,(S + b') = (S + a)\,(S + b)$.

Hence multiplication in R / S is also well defined.

Associativity of addition in R / S: We have

$$(S + a) + [(S + b) + (S + c)] = (S + a) + [S + (b + c)]$$
$$= S + [a + (b + c)] = S + [(a + b) + c] = [S + (a + b)] + (S + c)$$
$$= [(S + a) + (S + b)] + (S + c).$$

Commutativity of addition in R / S: We have

$$(S + a) + (S + b) = S + (a + b) = S + (b + a) = (S + b) + (S + a).$$

Existence of additive identity. We have $S = S + 0 \in R / S$.

If $S + a \in R / S$, then $(S + 0) + (S + a) = S + (0 + a) = S + a$.

$\therefore$ S is the additive identity.

Existence of additive inverse: Let $S + a \in R / S$.

Then $S + (-a) \in R / S$. Also we have

$$[S + (-a)] + [S + a] = S + [(-a) + a] = S + 0 = S.$$

$\therefore \quad S + (-a)$ or $S - a$ is the additive inverse of $S + a$.

Associativity of multiplication: We have

$$[(S + a)(S + b)](S + c) = (S + ab)(S + c) = S + (ab)c$$
$$= S + a(bc) = (S + a)(S + bc) = (S + a)[(S + b)(S + c)].$$

Distributivity of Multiplication with respect to Addition: We have

$$(S + a)[(S + b) + (S + c)] = (S + a)[S + (b + c)]$$
$$= S + a(b + c) = S + (ab + ac)$$
$$= (S + ab) + (S + ac)$$
$$= (S + a)(S + b) + (S + a)(S + c).$$

Similarly, we can prove that

$$[(S + b) + (S + c)](S + a) = (S + b)(S + a) + (S + c)(S + a).$$

Hence R/S is a ring with respect to the two compositions. The residue class $S + 0$ or S is the zero element of this ring.

Note: The students should not confuse that by the multiplication $(S + a)(S + b)$ of residue classes we mean the totality of elements obtained on multiplying the elements of $S + a$ with those of $S + b$. This multiplication of residue classes is a new composition which we have defined in the set R/S.

However the addition $(S + a) + (S + b)$ of residue classes as defined by us coincides with the totality of elements obtained on adding elements of $S + a$ to the elements of $S + b$ as can be easily seen :

$$(S + a) + (S + b) = S + (a + S) + b = S + (S + a) + b$$
$$= (S + S) + (a + b) = S + (a + b).$$

Illustrative Examples

Example 15: *If R/S is a ring of residue classes of S in R, prove that*

(i) If R is commutative, so also is R/S.

(ii) If R has a unity element 1 so also has R/S, namely $S + 1$. **(Gorakhpur 2014)**

Solution: (i) Suppose R is a commutative ring. Let $S + a, S + b$ be any two elements of R/S. Then $a, b \in R$ and $ab = ba$.

We have

$$(S + a)(S + b) = S + ab = S + ba = (S + b)(S + a).$$

(ii) Suppose R is a ring with unit element 1. Then $S + 1 \in R/S$. If $S + a$ is any element of R/S, we have

$$(S + 1)(S + a) = S + (1a) = S + a$$

and $$(S + a)(S + 1) = S + (a1) = S + a.$$

$\therefore$ $S + 1$ is the unit element of R/S.

11 Isomorphism of Rings

(Kumaun 2006)

A ring R is said to be isomorphic to another ring R' if there exists a one-one mapping f of R onto R' such that

$$f(a+b) = f(a) + f(b),\ f(ab) = f(a)\ f(b)\ \forall\ a, b \in R.$$

Also such a mapping f is said to be an isomorphism of R onto R'.

A mapping $f : R \to R'$ is an isomorphism of R onto R' if f is one-one onto and if $f(a+b) = f(a) + f(b),\ f(ab) = f(a)\ f(b)\ \forall\ a, b \in R$. For f to be an isomorphism of R onto R', it must be one-one onto and it must preserve both addition and multiplication compositions in R and R'. There may be more than one isomorphism of R onto R' if R is isomorphic to R'.

If a ring R is isomorphic to another ring R', we shall write in symbols $R \cong R'$. Also R' is said to be an isomorphic image of R.

Note: In the above definition of isomorphism of rings, we have denoted the compositions in the two rings by the same symbols. The elements tell us that what is the composition represented by any symbol. For example, $a, b \in R$. When we write $a + b$, ab then the respective compositions are addition and multiplication of R. Again $f(a), f(b) \in R'$. When we write $f(a) + f(b), f(a)\ f(b)$ then the respective compositions are addition and multiplication of R'.

Relation of isomorphism in the set of all rings:

As we have proved in groups, we can prove that the *relation of isomorphism in the set of all rings is an equivalence relation.* Therefore it will partition the set of all rings into disjoint equivalence classes such that any two rings of the same class are isomorphic to each other while rings of different classes are not isomorphic. Any two rings belonging to the same equivalence class are said to be **abstractly identical.**

Illustrative Examples

Example 16: *Let R be the ring of integers under ordinary addition and multiplication. Let R' be the set of all even integers. Let us define multiplication in R' to be denoted by $'*'$ by the relation $a * b = \frac{ab}{2}$,*

where ab is the ordinary multiplication of two integers a and b.

(i) Prove that $(R', +, *)$ is a commutative ring where $+$ stands for ordinary addition of integers.

(ii) Prove that R is isomorphic to R'. (iii) What acts as the unit element of R' ?

Solution: (i) Obviously R' is an abelian group with respect to addition.

If a and b are both even integers, then $\frac{ab}{2}$ is also an even integer.

Therefore, $a * b = \left(\frac{ab}{2}\right) \in R' \quad \forall \quad a, b \in R'$.

Thus R' is closed with respect to $*$.

Also if a, b, c are any elements of R', then

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = a \frac{(bc/2)}{2} = \frac{(ab/2)c}{2}$$

$$= \left(\frac{ab}{2}\right) * c = (a * b) * c$$

$\therefore$ $*$ is associative.

Further $a * b = \frac{ab}{2} = \frac{ba}{2} = b * a.$

$\therefore$ $*$ is commutative.

Again $a * (b + c) = \frac{a(b + c)}{2} = \frac{ab}{2} + \frac{ac}{2}$

$$= (a * b) + (a * c).$$

Similarly $(b + c) * a = (b * a) + (c * a)$.

$\therefore$ $*$ is distributive with respect to $+$.

$\therefore$ $(R', +, *)$ is a commutative ring.

(ii) We shall now show that R is isomorphic to R'. Consider the mapping f defined by

$$f : R \to R' \text{ such that } f(x) = 2x \quad \forall \quad x \in R.$$

The mapping f is obviously one-one onto.

Also $\forall \quad x_1, x_2 \in R$, we have

$$f(x_1 + x_2) = 2(x_1 + x_2) = 2x_1 + 2x_2 = f(x_1) + f(x_2)$$

and $f(x_1 x_2) = 2(x_1 x_2) = \frac{(2x_1)(2x_2)}{2}$

$$= (2x_1) * (2x_2) = f(x_1) * f(x_2).$$

$\therefore$ the mapping f is an isomorphism of R onto R'.

(iii) Here 1 is the unit element of R. We have $f(1) = 2$. Since f is an isomorphism of R onto R', therefore 2 must be the unit element of R'. We have for all

$$a \in R', 2 * a = \frac{2a}{2} = a = a * 2.$$

$\therefore$ 2 is the unit element of R'.

12 Properties of Isomorphism of Rings

Theorem: *If f is an isomorphism of a ring R onto a ring R', then*

(i) the image of the zero of R is the zero of R'.

(ii) the image of the negative of an element of R is the negative of the image of that element i.e., $f(-a) = -f(a) \quad \forall \quad a \in R$.

(iii) If R is a commutative ring, then R' is also a commutative ring.

(iv) If R is without zero divisors, then R' is also without zero divisors.

(v) If R is with unit element, then R' is also with unit element.

(vi) If R is a field, then R' is also a field.

(vii) If R is a skew field, then R' is also a skew field.

Proof: (i) Let $a \in R$. Then $f(a) \in R'$. Let $0'$ denote the zero element of R'. To prove that $f(0) = 0'$.

We have $f(a) + 0' = f(a) = f(a + 0) = f(a) + f(0)$. By cancellation law for addition in R', we get from $f(a) + 0' = f(a) + f(0)$, the result that $0' = f(0)$.

(ii) We have $f(a) + f(-a) = f[a + (-a)] = f(0) = 0'$.

$\therefore$ $f(-a)$ is the additive inverse of $f(a)$ in R'.

Thus $f(-a) = -f(a)$.

(iii) Let $f(a)$ and $f(b)$ be any two elements of R'. Then $a, b \in R$.

We have $f(a)\,f(b) = f(ab) = f(ba)$ [$\because$ R is commutative $\Rightarrow$ $ab = ba$]

$= f(b)\,f(a)$.

$\therefore$ R' is also commutative.

(iv) We have $f(0) = 0'$. Also f is one-one. Therefore 0 is the only element of R whose f-image is $0'$.

Let $f(a), f(b)$ be two non-zero elements of R'.

Then $f(a) \neq 0', f(b) \neq 0' \Rightarrow a \neq 0, b \neq 0$.

Since R is without zero divisors, therefore

$a \neq 0, b \neq 0 \Rightarrow ab \neq 0 \Rightarrow f(ab) \neq f(0)$

$\Rightarrow$ $f(a)\,f(b) \neq 0' \Rightarrow R'$ is without zero divisors.

(v) Let 1 be the unit element of R. Then $f(1) \in R'$. If $f(a)$ is any element of R', we have

$f(1)\,f(a) = f(1a) = f(a)$

and $f(a)\,f(1) = f(a1) = f(a)$.

$\therefore$ $f(1)$ is the unit element of R'.

(vi) If R is a field, then R is commutative, with unity and each non-zero element of R will possess multiplicative inverse. Now as proved in (iii) and (v), R' will be commutative and will also have the unit element *i.e.*, $f(1)$.

Let $f(a)$ be any non-zero element of R'. Then

$$f(a) \neq 0' \Rightarrow a \neq 0 \Rightarrow a^{-1} \text{ exists.}$$

Now $f(a^{-1}) \in R'$ and we have

$$f(a^{-1})\, f(a) = f(a^{-1}\, a) = f(1)$$

and $$f(a)\, f(a^{-1}) = f(aa^{-1}) = f(1).$$

$\therefore$ $f(a^{-1})$ is the multiplicative inverse of $f(a)$.

Hence R' is a field.

(vii) As shown in (v) R' will be with unit element *i.e.*, $f(1)$ and as shown in (vi) each non-zero element of R' will be inversible. Therefore R' is a skew-field.

Transference of Ring Structure:

Theorem: *If f is a one-one mapping of a ring R onto a set R' with two compositions denoted additively and multiplicatively such that*

$$f(a+b) = f(a) + f(b),\ f(ab) = f(a)\, f(b) \quad \forall\ a, b \in R,$$

then the set R' is a ring for the two compositions.

This theorem can be easily proved as we have proved the corresponding theorem on groups.

13 Imbedding of a Ring into another Ring

Definition: *A ring R is said to be imbedded in a ring R' if there is a subring S' of R' such that R is isomorphic to S'.*

Obviously a ring R can be imbedded in a ring R' if there exists a mapping f of R into R' such that f is one-to-one and

$$f(a+b) = f(a) + f(b),\ f(ab) = f(a)\, f(b) \quad \forall\ a, b \in R.$$

For then $f(R)$ is a subring of R' and f is an isomorphism of R onto $f(R)$ making R isomorphic to $f(R)$.

Theorem: *Any ring R without a unity element can be imbedded in a ring with unity.*

Proof: Let R be any ring without unity. Let Z be the ring of integers. Let

$$R' = R \times Z = \{(a, m) : a \in R \text{ and } m \in Z\}.$$

We shall show that when suitable binary operations have been defined in $R \times Z$, then it becomes a ring with a unity element containing a subring, isomorphic to R.

If (a, m) and (b, n) are two elements of $R \times Z$, then we define addition in $R \times Z$ by the equation

$$(a , m) + (b , n) = (a + b , m + n) \quad ...(1)$$

and multiplication in $R \times Z$ by the equation

$$(a , m)\,(b , n) = (ab + na + mb , mn). \quad ...(2)$$

In the right hand side of (1), $a + b$ is addition of two elements of R and $m + n$ is addition of two integers. In the right hand side of (2), ab is multiplication of two elements of R, mn is multiplication of two integers and na, mb are integral multiples of a and b which we have explained in article 3 of chapter 'Rings'.

Since $a + b \in R$ and $m + n \in Z$, therefore $(a + b , m + n) \in R \times Z$. Thus $R \times Z$ is closed with respect to addition. Further $ab , na , mb \in R \Rightarrow ab + na + mb \in R$. Also $mn \in Z$. Therefore $(ab + na + mb , mn) \in R \times Z$ and $R \times Z$ is closed with respect to multiplication.

Now let $(a , m), (b , n) , (c , p)$ be any elements of $R \times Z$. Then we observe:

Associativity of addition: We have

$$\begin{aligned}[(a , m) + (b , n)] + (c , p) &= (a + b , m + n) + (c , p)\\ &= ([a + b] + c , [m + n] + p)\\ &= (a + [b + c] , m + [n + p])\\ &= (a , m) + (b + c , n + p)\\ &= (a , m) + [(b , n) + (c , p)].\end{aligned}$$

Commutativity of addition: We have

$$\begin{aligned}(a , m) + (b , n) &= (a + b , m + n)\\ &= (b + a , n + m) \quad [\because \text{addition is commutative in } R \text{ and also in } Z]\\ &= (b , n) + (a , m).\end{aligned}$$

Existence of additive identity: We have $(0, 0) \in R \times Z$. Here the first 0 is the zero element of R and the second 0 is the zero integer. Also

$$(0 , 0) + (a , m) = (0 + a , 0 + m) = (a , m).$$

$\therefore$ $(0 , 0)$ is the additive identity.

Existence of additive inverse: If $(a , m) \in R \times Z$, then

$$(-a , -m) \in R \times Z$$

and we have

$$(-a , -m) + (a , m) = (-a + a , -m + m) = (0 , 0).$$

$\therefore$ $(-a , -m)$ is the additive inverse of (a , m).

Associativity of multiplication: We have

$$\begin{aligned}&[(a , m)\,(b , n)]\,(c , p) = (ab + na + mb , mn)\,(c , p)\\ &= ((ab + na + mb)\,c + p\,(ab + na + mb) + (mn)\,c , (mn)\,p)\\ &= (abc + n\,(ac) + m\,(bc) + p\,(ab) + (pn)\,a + (pm)\,b + (mn)\,c , (mn)\,p).\end{aligned}$$

Also $(a , m)\,[(b , n)\,(c , p)] = (a , m)\,(bc + pb + nc , np)$

$= (a\,(bc + pb + nc) + (np)\,a + m\,(bc + pb + nc) , m\,(np))$

$= (abc + a\,(pb) + a\,(nc) + (np)\,a + m\,(bc) + m\,(pb) + m\,(nc) , (mn)\,p)$

$= (abc + p\,(ab) + n\,(ac) + (np)\,a + m\,(bc) + (mp)\,b + (mn)\,c , (mn)\,p).$

We see that $[(a , m)\,(b , n)]\,(c , p) = (a , m)\,[(b , n)\,(c , p)].$

Distributive laws: We have

$(a , m)\,[(b , n) + (c , p)] = (a , m)\,(b + c , n + p)$

$= (a\,(b + c) + (n + p)\,a + m\,(b + c) , m\,(n + p))$

$= (ab + ac + na + pa + mb + mc , mn + mp)$

$= (ab + na + mb , mn) + (ac + pa + mc , mp)$

$= (a , m)\,(b , n) + (a , m)\,(c , p).$

Similarly we can show that the other distributive law also holds good.

Thus $R \times Z$ is a ring with respect to the operations defined on it.

Existence of multiplicative identity: We have $(0 , 1) \in R \times Z$. If $(a , m) \in R \times Z$, then

$(0 , 1)\,(a , m) = (0a + m0 + 1a , 1m) = (0 + 0 + a , m) = (a , m).$

Also $(a , m)\,(0 , 1) = (a0 + 1a + m0, m1) = (0 + a + 0, m) = (a, m).$

$\therefore$ $(0 , 1)$ is the multiplicative identity. So $R \times Z$ is a ring with unity element $(0, 1)$.

Now consider the subset $S' = R \times \{0\}$ of $R \times Z$ which consists of all pairs of the form $(a, 0)$. We shall show that $R \times \{0\}$ is a subring of $R \times Z$. Let $(a, 0), (b, 0)$ be any two elements of $R \times \{0\}$.

Then $(a, 0) - (b, 0) = (a, 0) + (- b, - 0) = (a - b, 0 - 0) = (a - b, 0)$

$\in R \times \{0\}.$

Also $(a, 0)\,(b, 0) = (ab + 0a + 0b, 00) = (ab + 0 + 0, 0)$

$= (ab, 0) \in R \times \{0\}.$

$\therefore$ $R \times \{0\}$ is a subring of $R \times Z$.

Finally we shall show that R is isomorphic to $R \times \{0\}$. Let ϕ be a mapping from R to $R \times \{0\}$ defined as $\phi\,(a) = (a, 0)\ \forall\ a \in R$.

ϕ is one-one: We have

$\phi\,(a) = \phi\,(b) \Rightarrow (a, 0) = (b, 0)$

$\Rightarrow$ $a = b \Rightarrow \phi$ is one-one.

ϕ is onto: Let $(a, 0)$ be any element of $R \times \{0\}$. Then $a \in R$ and we have $\phi\,(a) = (a, 0)$.

Therefore ϕ is onto.

ϕ preserves additions and multiplications:

If a, b be any two elements of R, then

$$\phi(a+b) = (a+b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b).$$

Also $\phi(ab) = (ab, 0) = (a, 0)(b, 0) = \phi(a)\,\phi(b)$.

$\therefore$ ϕ preserves compositions.

Hence ϕ is an isomorphism of R onto $R \times \{0\}$.

This completes the proof of the theorem.

14 The Field of Quotients

Definition: *A ring R can be imbedded in a ring S if S contains a subset S′ such that R is isomorphic to S′.*

If D is a commutative ring without zero divisors, then we shall see that it can be imbedded in a field F *i.e.,* there exists a field F which contains a subset D' isomorphic to D. We shall construct a field F with the help of elements of D and this field F will contain a subset D' such that D is isomorphic to D'. This field F is called the **'field of quotients'** of D, or simply the *'quotient field'* of D.

On account of isomorphism of D onto D', we can say that D and D' are abstractly identical. Therefore if we identify D' with D, then we can say that the quotient field F of D is a field containing D. We shall also see that F is the smallest field containing D.

Motivation for the construction of the quotient field: We are all quite familiar with the ring **I** of integers. Also our familiar set **Q** of rational numbers is nothing but the set of quotients of the elements of **I**. Thus

$$\mathbf{Q} = \left\{ \frac{p}{q} : p \in \mathbf{I}, 0 \neq q \in \mathbf{I} \right\}.$$

If we identify the rational numbers..., $\frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \ldots$ with the integers ..., $-3, -2, -1, 0, 1, 2, 3, \ldots$, then $\mathbf{I} \subseteq \mathbf{Q}$.

Also $(\mathbf{Q}, +, .)$ is a field. It is the smallest field containing **I**.

Also if $\frac{a}{b}$ and $\frac{c}{d} \in \mathbf{Q}$, then we remember that

(i) $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$, (ii) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, (iii) $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain. We have the following theorem:

Theorem 1: *A commutative ring with zero divisors can be imbedded in a field.*

Or

Every integral domain can be imbedded in a field.

Or

From the elements of an integral domain D, it is possible to construct a field F which contains a subset D′ isomorphic to D.

Proof: Let D be a commutative ring without zero divisors. Let D_0 be the set of all non-zero elements of D. Let $S = D \times D_0$ *i.e.,* let S be the set of all ordered pairs (a, b) where $a, b \in D$ and $b \neq 0$. Let us define a relation $\sim$ in S. We shall say that $(a , b) \sim (c , d)$ if and only if $ad = bc$.

We claim that this relation is an equivalence relation in S.

Reflexivity: Since D is a commutative ring, therefore $ab = ba \ \forall \ a , b \in D$. Therefore $(a, b) \sim (a, b) \ \forall \ (a, b) \in S$.

Symmetry: We have $(a, b) \sim (c, d)$

$\Rightarrow$ $ad = bc \Rightarrow da = cb$ [$\because$ Multiplication is commutative in D]

$\Rightarrow$ $cb = da \Rightarrow (c , d) \sim (a , b)$.

Transitivity: Let $(a , b) \sim (c , d)$ and $(c , d) \sim (e , f)$.

Then $ad = bc$ and $cf = de$.

$\therefore$ $adf = bcf$ and $bcf = bde$.

$\therefore$ $adf = bde$

$\Rightarrow$ $afd = bed$ [$\because$ D is a commutative ring]

$\Rightarrow$ $afd - bed = 0 \Rightarrow (af - be)\, d = 0$

$\Rightarrow$ $af - be = 0$ [$\because d \neq 0$ and D is without zero divisors]

$\Rightarrow$ $af = be \Rightarrow (a , b) \sim (e , f)$.

Thus $\sim$ is an equivalence relation in S. Therefore it will partition S into disjoint equivalence classes. We shall denote the equivalence class containing (a , b) by $\frac{a}{b}$. Other notations to denote this equivalence class are $\overline{(a , b)}$ or $[a , b]$.

Then $\frac{a}{b} = \{(c , d) \in S : (c , d) \sim (a , b)\}$.

Obviously $\frac{a}{b} = \frac{c}{d}$ iff $(a , b) \sim (c , d)$ *i.e.,* iff $ad = bc$.

Also $\frac{a}{b} = \frac{ax}{bx} \ \forall \ x \in D_0$. The reason is that $(a, b) \sim (ax, bx)$ since $abx = bax$.

These equivalence classes are our quotients. Let F be the set of all such quotients

i.e., $F = \left\{\frac{a}{b} : (a, b) \in S\right\}$.

We now define addition and multiplication operations in F as follows :

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ and } \frac{a}{b}\,\frac{c}{d}=\frac{ac}{bd}\cdot$$

Since D is without zero divisors, therefore $b\neq 0, d\neq 0 \Rightarrow bd\neq 0$.

Therefore both $\frac{ad+bc}{bd}$ and $\frac{ac}{bd}$ are elements of F. Thus F is closed with respect to addition and multiplication. We shall now show that both addition and multiplication in F are well defined. For this we are to show that if

$$\frac{a}{b}=\frac{a'}{b'} \text{ and } \frac{c}{d}=\frac{c'}{d'}\text{, then } \frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'} \text{ and } \frac{a}{b}\,\frac{c}{d}=\frac{a'}{b'}\,\frac{c'}{d'}\cdot$$

We have $\frac{a}{b}=\frac{a'}{b'}\Rightarrow ab'=ba'$ and $\frac{c}{d}=\frac{c'}{d'}\ \Rightarrow\ cd'=dc'$.

Now to show that $\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}$, we are to show that

$$\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'} \text{ i.e., } (ad+bc)\,b'\,d'=bd\,(a'd'+b'c').$$

Now
$$\begin{aligned}(ad+bc)\,b'd' &= adb'd'+bcb'd'=ab'dd'+bb'cd'\\ &= ba'dd'+bb'dc' \qquad [\because\ ab'=ba' \text{ and } cd'=dc']\\ &= bda'd'+bdb'c'=bd\,(a'd'+b'c'),\end{aligned}$$

which was desired.

Again to show that $\frac{a}{b}\,\frac{c}{d}=\frac{a'}{b'}\,\frac{c'}{d'}$ we are to show that

$$\frac{ac}{bd}=\frac{a'c'}{b'd'}, \text{ i.e., } acb'd'=bda'c'.$$

Now $acb'd'=ab'cd'=ba'dc'=bda'c'$, which was desired.

Therefore both addition and multiplication are well defined on F. We shall now show that F is a field for these two operations.

Associativity of addition: We have

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)\,f+bde}{bdf}$$

$$=\frac{adf+bcf+bde}{bdf}=\frac{adf+b\,(cf+de)}{bdf}=\frac{a}{b}+\frac{cf+de}{df}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)\cdot$$

Commutativity of addition: We have

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}\cdot$$

Existence of additive identity: We have $\frac{0}{a}\in F$ where $a\neq 0$. If $\frac{c}{d}$ is any element of F, then

$$\frac{0}{a}+\frac{c}{d}=\frac{0d+ac}{ad}=\frac{0+ac}{ad}=\frac{ac}{ad}=\frac{c}{d}. \qquad [\because acd = adc]$$

$\therefore$ $\frac{0}{a}$ is the additive identity. It should be noted that

$$\frac{0}{a}=\frac{0}{b}\ \forall a,b\in D_0. \text{ Also } \frac{c}{d}=\frac{0}{a} \text{ iff } ca = d\,0 \text{ } i.e., \text{ } c = 0.$$

Existence of additive inverse: If $\frac{a}{b}\in F$, then $\frac{-a}{b}\in F$.

Also we have, $\frac{-a}{b}+\frac{a}{b}=\frac{(-a)\,b+ba}{b^2}=\frac{0}{b^2}=\frac{0}{a}$ $\qquad [\because 0a = b^2\,0]$

$\therefore$ $\frac{-a}{b}$ is the additive inverse of $\frac{a}{b}$.

Associativity of multiplication: We have

$$\left(\frac{a}{b}\,\frac{c}{d}\right)\frac{e}{f}=\frac{ac}{bd}\,\frac{e}{f}=\frac{(ac)\,e}{(bd)\,f}=\frac{a\,(ce)}{b\,(df)}=\frac{a}{b}\,\frac{ce}{df}=\frac{a}{b}\left(\frac{c}{d}\,\frac{e}{f}\right).$$

Commutativity of multiplication: We have

$$\frac{a}{b}\,\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\,\frac{a}{b}.$$

Existence of multiplicative identity: We have

$\frac{a}{a}\in F$ where $a \neq 0$. Also if $\frac{c}{d}\in F$, then

$$\frac{a}{a}\,\frac{c}{d}=\frac{a}{a}\,\frac{c}{d}=\frac{c}{d} \qquad [\because (ac, ad) \sim (c, d) \text{ because } acd = adc]$$

$\therefore$ $\frac{a}{a}$ is the multiplicative identity. It should be noted that

$$\frac{a}{a}=\frac{b}{b}\ \forall\ a, b\in D_0.$$

Existence of multiplicative inverse of non-zero elements of F:

Let $\frac{a}{b}$ be any non-zero element of F. Then $a \neq 0$.

$\therefore$ $\frac{b}{a}\in F$. Also we have

$$\frac{a}{b}\,\frac{b}{a}=\frac{ab}{ba}=\frac{ab}{ab}=\frac{a}{a}= \text{ the unity element.}$$

$\therefore$ $\frac{b}{a}$ is the multiplicative inverse of $\frac{a}{b}$.

Distributivity of multiplication over addition: We have

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\,\frac{cf+de}{df}=\frac{a\,(cf+de)}{bdf}=\frac{acf+ade}{bdf}$$

$$= \frac{(acf + ade)\, bdf}{bdf\ bdf} = \frac{acf\ bdf + bdf\ ade}{bdf\ bdf}$$

$$= \frac{acf}{bdf} + \frac{ade}{bdf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}.$$

Similarly the other distributive law holds.

$\therefore$ F is a field under the addition and multiplication as defined above. This field F is called the field of quotients of D.

We shall now show that the field F contains a subset D' such that D is isomorphic to D'.

Let $D' = \left\{\frac{ax}{x} \in F : a, 0 \neq x \in D\right\}$. Then $D' \subseteq F$. If $x \neq 0$, $y \neq 0$ are elements of D, then $\frac{ax}{x} = \frac{ay}{y}$ since $axy = xay$. Therefore if x is any fixed non-zero element of D, we can write

$$D' = \left\{\frac{ax}{x} \in F : a \in D\right\}.$$

We claim that the function $\phi : D \to D'$ defined by

$$\phi(a) = \frac{ax}{x} \quad \forall\ a \in D \text{ is an isomorphism of } D \text{ onto } D'.$$

ϕ is one-one: We have

$$\phi(a) = \phi(b) \Rightarrow \frac{ax}{x} = \frac{bx}{x} \Rightarrow axx = xbx \Rightarrow ax^2 = bx^2 \Rightarrow (a - b)\, x^2 = 0$$

$\Rightarrow$ $a - b = 0$, since $x^2 \neq 0$

$\Rightarrow$ $a = b$.

$\therefore$ ϕ is one-one.

ϕ is onto D': If $\frac{ax}{x} \in D'$, then $a \in D$. Also we have $\phi(a) = \frac{ax}{x}$.

Thus ϕ is onto D'.

Also
$$\phi(a + b) = \frac{(a + b)\, x}{x} = \frac{(a + b)\, x^2}{x^2}$$
$$= \frac{ax^2 + bx^2}{x^2} = \frac{axx + xbx}{x^2}$$
$$= \frac{ax}{x} + \frac{bx}{x} = \phi(a) + \phi(b)$$

and
$$\phi(ab) = \frac{(ab)\, x}{x} = \frac{(ab)\, x^2}{x^2} = \frac{(ax)\,(bx)}{x^2} = \frac{ax}{x}\frac{bx}{x}$$
$$= \phi(a)\, \phi(b).$$

$\therefore$ ϕ is an isomorphism of D onto D'.

Hence $D \cong D'$.

If we identify D' with D *i.e.,* if in F we write a, b, c etc. in place of $\frac{ax}{x}, \frac{bx}{x}, \frac{cx}{x}$ etc., then we see that D is contained in F. Thus F (the field of quotients of D) is a field containing D.

In the next theorem we shall show that the quotient field F of D is the smallest field containing D. In other words if D is contained in any other field K, then F will also be contained in K.

Theorem 2: *If K is any field which contains an integral domain D, then K contains a subfield isomorphic to the quotient field F of D.*

In other words the quotient field F of D is the smallest field containing D.

Proof: Let D be a commutative ring without zero divisors. Let $a \in D$ and $0 \neq b \in D$. Since K is a field containing D, therefore

$$a \in K, 0 \neq b \in K \Rightarrow ab^{-1} \in K.$$

Let K' be the subset of K containing the elements of the form ab^{-1} where $a, b \in D$ with $b \neq 0$. Thus

$$K' = \{ab^{-1} \in K : a, 0 \neq b \in D\}.$$

We shall show that K' is a subfield of K and K' is isomorphic to the quotient field F of D. Let $ab^{-1} \in K', cd^{-1} \in K'$. Then

$$0 \neq b, 0 \neq d \in D.$$

Now
$$ab^{-1} - cd^{-1} = add^{-1}b^{-1} - cbb^{-1}d^{-1} = (ad - bc)\, d^{-1}b^{-1}$$
$$= (ad - bc)\, (bd)^{-1} \in K',$$

since $ad - bc \in D$ and $0 \neq bd \in D$.

Further suppose that $0 \neq cd^{-1} \in K'$. Then $c \neq 0$ and we have

$$(ab^{-1})\, (cd^{-1})^{-1} = ab^{-1}dc^{-1} = ad\, (cb)^{-1} \in K',$$

since $ad \in D$ and $0 \neq cb \in D$.

Hence K' is a subfield of K. We shall now show that the quotient field F of D is isomorphic to K'. We have

$$F = \left\{\frac{a}{b} : a \in D, 0 \neq b \in D\right\}.$$

Consider the mapping $f : F \to K'$ defined by

$$f\left(\frac{a}{b}\right) = ab^{-1} \; \forall \frac{a}{b} \in F.$$

The mapping f is one-one because we have

$$f\left(\frac{a}{b}\right) = f\left(\frac{c}{d}\right) \Rightarrow ab^{-1} = cd^{-1}$$

$\Rightarrow \quad ab^{-1}bd = cd^{-1}bd \Rightarrow ad = cb\ d^{-1}d$

$\Rightarrow \quad ad = bc \Rightarrow (a, b) \sim (c, d) \Rightarrow \frac{a}{b} = \frac{c}{d}$.

Also f is onto K'. If ab^{-1} is any element of K', then

$$\frac{a}{b} \in F \text{ and } f\left(\frac{a}{b}\right) = ab^{-1}.$$

Further
$$f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{ad + bc}{bd}\right) = (ad + bc)\,(bd)^{-1}$$
$$= (ad + bc)\,d^{-1}b^{-1} = add^{-1}b^{-1} + bc\,d^{-1}b^{-1}$$
$$= ab^{-1} + cd^{-1} = f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right).$$

Also
$$f\left(\frac{a}{b}\,\frac{c}{d}\right) = f\left(\frac{ac}{bd}\right) = (ac)\,(bd)^{-1} = (ac)\,d^{-1}\,b^{-1}$$
$$= (ab^{-1})\,(cd^{-1}) = f\left(\frac{a}{b}\right) f\left(\frac{c}{d}\right).$$

Hence $F \cong K'$.

If we identify K' with F, we see that if D is contained in any field K, then F is also contained in K. Therefore F is the smallest field containing D.

Corollary: *The quotient field of a finite integral domain coincides with itself.*

Suppose D is a finite integral domain. Then D is also a field. Thus D is the smallest field containing D. The quotient field F of D is also the smallest field containing D. Hence F coincides with D.

Theorem3: *Any two isomorphic integral domains have isomorphic quotient fields.*

Proof: Suppose D and D' are two isomorphic integral domains.

Let f be an isomorphism of D onto D'. If a, b, c etc. are the elements of D then $f(a), f(b), f(c)$ etc. will be the elements of D'. Also

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)\,f(b)\ \forall\ a, b \in D.$$

Let F, F' be the quotient fields of D, D' respectively. Then F consists of the equivalence classes (quotients) of the form $\frac{a}{b}$ where $a, 0 \neq b \in D$ and F' consists of the equivalence classes of the form $\frac{f(a)}{f(b)}$ where $f(a), 0 \neq f(b) \in D'$.

Consider the mapping $\phi : F \to F'$ defined by

$$\phi\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)} \quad \forall \quad \frac{a}{b} \in F.$$

First we shall show that the mapping ϕ is well defined *i.e.,* if $\frac{a}{b} = \frac{c}{d}$, then

$$\phi\left(\frac{a}{b}\right) = \phi\left(\frac{c}{d}\right).$$

We have $\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$

$\Rightarrow$ $f(ad) = f(bc) \Rightarrow f(a)\, f(d) = f(b)\, f(c)$

$\Rightarrow$ $\frac{f(a)}{f(b)} = \frac{f(c)}{f(d)} \Rightarrow \phi\left(\frac{a}{b}\right) = \phi\left(\frac{c}{d}\right).$

$\therefore$ ϕ is well-defined.

ϕ is one-one: We have

$$\phi\left(\frac{a}{b}\right) = \phi\left(\frac{c}{d}\right) \Rightarrow \frac{f(a)}{f(b)} = \frac{f(c)}{f(d)}$$

$\Rightarrow$ $f(a)\, f(d) = f(b)\, f(c) \Rightarrow f(ad) = f(bc)$

$\Rightarrow$ $ad = bc$ [$\because f$ is one-one]

$\Rightarrow$ $\frac{a}{b} = \frac{c}{d}$.

$\therefore$ ϕ is one-one.

Also ϕ is onto F'. If $\frac{f(a)}{f(b)} \in F'$, then

$\frac{a}{b} \in F$ and $\phi\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$. Therefore ϕ is onto F'.

Further $$\phi\left(\frac{a}{b} + \frac{c}{d}\right) = \phi\left(\frac{ad + bc}{bd}\right) = \frac{f(ad + bc)}{f(bd)} = \frac{f(ad) + f(bc)}{f(b)\, f(d)}$$

$$= \frac{f(a)\, f(d) + f(b)\, f(c)}{f(b)\, f(d)} = \frac{f(a)}{f(b)} + \frac{f(c)}{f(d)}$$

$$= \phi\left(\frac{a}{b}\right) + \phi\left(\frac{c}{d}\right).$$

Also $$\phi\left(\frac{a}{b}\,\frac{c}{d}\right) = \phi\left(\frac{ac}{bd}\right) = \frac{f(ac)}{f(bd)} = \frac{f(a)\, f(c)}{f(b)\, f(d)}$$

$$= \frac{f(a)}{f(b)}\,\frac{f(c)}{f(d)} = \phi\left(\frac{a}{b}\right)\phi\left(\frac{c}{d}\right).$$

$\therefore$ ϕ is an isomorphism of F onto F'.

$\therefore$ $F \cong F'$.

15 Divisibility in an Integral Domain

Definition: *Suppose $0 \neq a$ is an element of a commutative ring R. Then a is said to divide $b \in R$, if there exists an element $c \in R$ such that $b = ca$.*

We shall use the symbol $a \mid b$ to represent the fact that a divides b. Also if a divides b then sometimes we say that a is a factor of b or b is divisible by a or a is a divisor of b. From the definition of divisibility it follows that every non-zero element of R is a divisor of its zero element. Obviously we can write $0 = a0$. Therefore if $0 \neq a \in R$, then $a \mid 0$.

Illustration 1: *In the ring* **I** *of integers, we have* $3 \mid 6$ *since we have* $6 = 3 \times 2$ *and* $2 \in \mathbf{I}$.

However in the ring of integers 3 is not a divisor of 7.

Illustration 2: *In the ring* **Q** *of rational numbers, we have* $3 \mid 7$ *since we have* $7 = 3 \times (7 / 3)$ *and* $7 / 3 \in \mathbf{Q}$.

Theorem 1: *If R is a commutative ring, then*

(i) $a \mid b$ *and* $b \mid c \Rightarrow a \mid c$ *i.e., the relation of divisibility in R is a transitive relation.*

(ii) $a \mid b$ *and* $a \mid c \Rightarrow a \mid (b + c)$.

(iii) $a \mid b \Rightarrow a \mid bx$ *for all* $x \in R$.

Proof: (i) $a \mid b \Rightarrow b = ap$ for some $p \in R$

and $b \mid c \Rightarrow c = bq$ for some $q \in R$.

Now $c = bq$ and $b = ap \Rightarrow c = (ap)\, q \Rightarrow c = a\,(pq)$

$\Rightarrow a \mid c$ since $pq \in R$.

(ii) $a \mid b \Rightarrow b = ap$ for some $p \in R$

and $a \mid c \Rightarrow c = aq$ for some $q \in R$.

Now $b = ap$ and $c = aq \Rightarrow b + c = ap + aq \Rightarrow b + c = a\,(p + q)$

$\Rightarrow a \mid (b + c)$ since $(p + q) \in R$.

(iii) $a \mid b \Rightarrow b = ap$ for some $p \in R$.

Now $b = ap \Rightarrow bx = (ap)\, x \quad \forall \quad x \in R$

$\Rightarrow bx = a\,(px) \Rightarrow a \mid bx$ since $px \in R$.

16 Units

Definition: *Let R be a commutative ring with unity element* 1. *An element $a \in R$ is a unit in R if there exists an element $b \in R$ such that $ab = 1$.*

In other words units of R are those elements of R which possess multiplicative inverse.

The students should not confuse a unit with the unit element or the unity element of the ring. There may be more than one units in a ring but the unity element is always unique. Of course the unity element is also one of the units.

In the ring of integers **I**, the only units are 1 and -1. These are the only inversible elements of the ring of integers.

Every non-zero element of a field possesses multiplicative inverse. Therefore every non-zero element of a field is a unit.

It is obvious that if a is a unit in a ring R, then a^{-1} is also a unit in R. Also the product of two units is again a unit. Because if a, b are two units in R, then $(ab)^{-1} = b^{-1}\ a^{-1}$ which is an element of R. Of course *the set of all units in R forms a group under multiplication.*

Illustrative Examples

Example 17: *Find all the units of the integral domain of Gaussian integers.*

Solution: Let $D = \{a + ib : a, b \in \mathbf{I}$, the set of integers$\}$ be the ring of Gaussian integers. The element $1 + 0\ i$ is the unity element of this ring. Let $x + iy$ be a unit and $x' + iy'$ be its inverse.

Then $(x + iy)(x' + iy') = 1 + 0\ i$

or $(xx' - yy') + i(xy' + yx') = 1 + 0\ i.$

Equating real and imaginary parts, we get

$$xx' - yy' = 1 \qquad ...(1)$$

and $$xy' + yx' = 0. \qquad ...(2)$$

Squaring and adding (1) and (2), we get

$$x^2 x'^2 + y^2 y'^2 + x^2 y'^2 + y^2 x'^2 = 1$$

or $$(x^2 + y^2)(x'^2 + y'^2) = 1.$$

Now the product of two positive integers can be equal to 1 if and only if each of them is 1.

$\therefore$ $x^2 + y^2 = 1$..

This gives $x^2 = 0, y^2 = 1$

or $x^2 = 1, y^2 = 0.$

Thus $x = 0, y = \pm 1$

or $x = \pm 1, y = 0.$

$\therefore$ The only units of the integral domain of Gaussian integers are

$$0 \pm i, (\pm 1) + 0i$$

i.e., $1, -1, i, -i.$

17 Associates

Definition: *Let R be a commutative ring with unity element* 1. *Then an element a of R is said to be an associate of* $b \in R$ *if* $a = ub$ *for some unit u in R.*

In symbols, we express it by writing $a \sim b$ which is read as '*a* is an associate of *b*' or '*a* and *b* are associates'.

From this definition we observe that in a commutative ring with unity all the associates of an element can be obtained by multiplying that element by different units in that ring.

Illustrations:

1. The only units of the integral domain of integers are 1 and -1. Therefore if a is any non-zero integer, then it has exactly two associates namely $1a$ and $(-1)\,a$ *i.e.,* a and $-a$. Thus the two associates of 5 are 5 and -5.
2. In any commutative ring with unity the associate of 0 is only zero.
3. The only units of the domain of Gaussian integers are $1, -1, i, -i$. Therefore if $a + ib$ is any non-zero element of this domain, then it has exactly four associates namely,

$$1(a + ib), -1(a + ib), i(a + ib), -i(a + ib)$$

i.e., $$a + ib, -a - ib, -b + ia, b - ia.$$

Theorem 2: *Let R be a commutative ring with unity element* 1. *The relation in R defined by 'a is an associate of b' is an equivalence relation.*

Proof:

Reflexivity: Let a be any element of R. Then $a = 1a$. Therefore $a \sim a$ because 1 is a unit in R. Thus $\sim$ is reflexive.

Symmetry: We have $a \sim b \Rightarrow a = ub$ for some unit u in R

$$\Rightarrow u^{-1}a = u^{-1}ub \Rightarrow u^{-1}a = 1b \Rightarrow u^{-1}a = b \Rightarrow b = u^{-1}a \Rightarrow b \sim a$$

because u^{-1} is also a unit in R. Therefore $\sim$ is symmetric.

Transitivity: Let $a \sim b, b \sim c$. Then $a = ub$ and $b = vc$ for some units $u, v \in R$. This gives $a = u(vc) = (uv)c$. But the product of two units in R is again a unit in R. Therefore uv is a unit in R and so $a = (uv)c \Rightarrow a \sim c$. Therefore $\sim$ is transitive.

Hence $\sim$ is an equivalence relation in R.

Theorem 3: *Let D be an integral domain with unity element* 1. *Two non-zero elements* $a, b \in D$ *are associates if and only if* $a \mid b$ *and* $b \mid a$.

Proof: Let two non-zero elements a, b be associates of each other in D. Then $a = bu$ where u is a unit in D.

Now $a = bu \Rightarrow b \mid a$.
Again $a = bu \Rightarrow au^{-1} = buu^{-1} \Rightarrow au^{-1} = b \Rightarrow b = au^{-1} \Rightarrow a \mid b$.

Thus a and b are associates $\Rightarrow a \mid b$ and $b \mid a$.

Conversely, let $a \mid b$ and $b \mid a$. Then to prove that a and b are associates.

We have $a \mid b \Rightarrow \exists\, c \in D$ such that $b = ac$.
Similarly $b \mid a \Rightarrow \exists\, d \in D$ such that $a = bd$.
$\therefore$ $b = ac = (bd)\, c = b\,(dc)$.
$\therefore$ $b1 = b\,(dc)$ $[\because\ b1 = b]$
or $b\,(1 - dc) = 0$
or $1 - dc = 0$ $[\because b \neq 0$ and D is without zero divisors$]$
or $1 = dc$.

$\therefore$ both c and d are units in D.

Thus $a = bd$ where d is a unit in D. Hence a and b are associates.

Note: In a field any two non-zero elements are associates.

18 Proper and Improper Divisors

Definition: *Let D be an integral domain with unity element 1. Let a be any non-zero element of D. Then the units of D and the associates of a are always divisors of a. These are called improper or trivial divisors of a. Any other divisors of a are called proper or non-trivial divisors of a.*

In the integral domain of integers $\pm 1, \pm 6$ are trivial divisors of 6. But $\pm 2, \pm 3$ are proper divisors of 6.

19 Prime Elements

Definition: *Let D be an integral domain with unity element 1. A non-zero non-unit element $a \in D$, having only trivial divisors, is called a* **prime** *or* **irreducible** *element of D.*

An element $0 \neq b \in D$ having proper divisors is called a **reducible or composite** element of D. From this definition it is obvious that if p is a prime element of D and if $p = xy$, where $x, y \in D$, then one of x or y must be unit in D.

Also $0 \neq b \in D$ is a composite element of D if and only if we can find two elements $x, y \in D$ such that $b = xy$ and none of x and y is a unit in .

20 Greatest Common Divisor

Definition: *Let R be a commutative ring. If $a, b \in R$, then $0 \neq d \in R$ is said to be a greatest common divisor of a and b if*

(i) $d \mid a$ *and* $d \mid b$.

(ii) Whenever $c \mid a$ and $c \mid b$ then $c \mid d$.

We shall use the notation $d = (a, b)$ to denote that d is a greatest common divisor of a and b.

Now suppose $a, b \in D$ where D is an integral domain with unity element 1. Let a, b possess a greatest common divisor.

If d_1, d_2 are two greatest common divisors of a and b, we have

$$d_1 \mid d_2 \text{ and } d_2 \mid d_1$$

$\Rightarrow$ d_1 and d_2 are associates.

Thus in an integral domain with unity in case a greatest common divisor of a and b exists, it is unique apart from the distinction between associates.

21 Relatively Prime Elements

Definition: *Let D be an integral domain with unity element 1. Two elements $a, b \in D$ are said to be relatively prime if their greatest common divisor is a unit of D.*

But any associate of a greatest common divisor is a greatest common divisor. Also the unity element 1 is an associate of any unit. Therefore if a, b are relatively prime we may assume that a greatest common divisor of a and b is 1 *i.e.,* $(a, b) = 1$.

22 Homomorphisms of Rings

Definition: **(Gorakhpur 2012)**

Homomorphism into: *A mapping f from a ring R into a ring R' is said to be a homomorphism of R into R' if*

(i) $f(a + b) = f(a) + f(b) \quad \forall \ a, b \in R$

(ii) $f(ab) = f(a)\, f(b)$ *for all* $a, b \in R$.

Homomorphism onto: *A mapping f from a ring R onto a ring R' is said to be a homomorphism of R onto R' if*

(i) $f(a + b) = f(a) + f(b) \quad \forall \ a, b \in R$.

(ii) $f(ab) = f(a)\, f(b) \quad \forall \ a, b \in R$.

Also then R' is said to be a homomorphic image of R.

Theorem 1: *If f is a homomorphism of a ring R into a ring R', then*

(i) $f(0) = 0'$, *where* 0 *is the zero element of the ring R and* $0'$ *is the zero element of* R'.

(ii) $f(-a) = -f(a) \quad \forall \ a \in R$. **(Gorakhpur 2011)**

Proof: (i) Let $a \in R$. Then $f(a) \in R'$. We have

$$f(a) + 0' = f(a) \qquad [\because\ 0' \text{ is the additive identity of } R']$$
$$= f(a + 0) = f(a) + f(0).$$

Now R' is a group with respect to addition. Therefore

$$f(a) + 0' = f(a) + f(0)$$
$$\Rightarrow \qquad 0' = f(0). \qquad [\text{By left cancellation law}]$$

(ii) Let a be any element of R. Then $-a \in R$.

We have $\quad 0' = f(0) = f[a + (-a)] = f(a) + f(-a)$.

$\therefore$ $f(-a)$ is the additive inverse of $f(a)$ in the ring R'. Thus

$$f(-a) = -f(a).$$

Theorem 2: *Let ϕ be a homomorphic mapping of a ring R into a ring R'. Let S' be the homomorphic image of R in R'. Then S' is a subring of R'.*

Proof: Since S' is the image of R in R' under the mapping ϕ, therefore

$$\phi(R) = S' \subseteq R'.$$

Let a', b' be any two elements of S'. Since $S' = \phi(R)$, therefore there exist elements $a, b \in R$ such that $\phi(a) = a'$, $\phi(b) = b'$.

We have $\quad a' - b' = \phi(a) - \phi(b) = \phi(a - b).$ $\qquad [\because\ \phi \text{ is a homomorphism}]$

Now $a - b \in R$ is such that $a' - b' = \phi(a - b)$. Therefore

$$a' - b' \in S'.$$

Further $\quad a'b' = \phi(a)\,\phi(b) = \phi(ab) \in S'$, since $ab \in R$.

Thus $\quad a', b' \in S' \Rightarrow a' - b' \in S'$ and $a'b' \in S'$.

Therefore S' is a subring of R'.

23 Kernel of a Ring Homomorphism

(Kumaun 2010, 12)

Definition: *If f is a homomorphism of a ring R into a ring R', then the set S of all those elements of R which are mapped onto the zero element of R' is called the kernel of the homomorphism f.*

Thus if f is a homomorphism of R into R', then S is the kernel of f if

$$S = \{x \in R : f(x) = 0' \text{ where } 0' \text{ is the zero element of } R'\}$$

Theorem 1: *If f is a homomorphism of a ring R into a ring R' with kernel S, then S is an ideal of R.* **(Gorakhpur 2011)**

Proof: Let f be a homomorphism of a ring R into a ring R'. Let $0, 0'$ be the zero elements of R, R' respectively. Let S be the kernel of f. Then

$$S = \{x \in R : f(x) = 0'\}$$

Since $f(0) = 0'$, therefore at least $0 \in S$. Thus S is not empty.

Let $a, b \in S$. Then $f(a) = 0'$, $f(b) = 0'$.

We have $f(a - b) = f[a + (-b)] = f(a) + f(-b)$

$= f(a) - f(b) = 0' - 0' = 0'$.

$\therefore$ $a - b \in S$.

Also if r be any element of R, then

$f(ar) = f(a)\, f(r) = 0'\, f(r) = 0'$

and $f(r\,a) = f(r)\, f(a) = f(r)0' = 0'$.

$\therefore$ $ar \in S$, $r\,a \in S$.

Thus $a, b \in S$, $r \in R \Rightarrow (a - b) \in S$, $a\,r \in S$, $r\,a \in S$.

$\therefore$ S is an ideal of R.

Theorem 2: *The homomorphism ϕ of a ring R into a ring R' is an isomorphism of R into R' if and only if $I(\phi) = (0)$, where $I(\phi)$ denotes the kernel of ϕ.*

Proof: Let ϕ be a homomorphism of a ring R into a ring R'. Let $0, 0'$ be the zero elements of R, R' respectively. Let $S = I(\phi)$ be kernel of ϕ. Then S is an ideal of R and

$S = \{a \in R : \phi(a) = 0'\}$.

Suppose ϕ is an isomorphism of a ring R into R'. Then ϕ is one-one. Let $a \in S$. Then

$\phi(a) = 0'$ [by def. of kernel]

$\Rightarrow$ $\phi(a) = \phi(0)$ [$\because$ $\phi(0) = 0$]

$\Rightarrow$ $a = 0$. [$\because$ ϕ is one-one]

Thus $a \in S \Rightarrow a = 0$. In other words 0 is the only element of R which belongs to S. Therefore $S = (0)$.

Conversely suppose that $S = (0)$. Then to prove that ϕ is an isomorphism of R into R' *i.e.*, to prove that ϕ is one-one.

If $a, b \in R$, then $\phi(a) = \phi(b)$

$\Rightarrow$ $\phi(a) - \phi(b) = 0'$ [$\because$ $\phi(a), \phi(b)$ are in the ring R']

$\Rightarrow$ $\phi(a - b) = 0'$ [$\because$ ϕ is a homomorphism]

$\Rightarrow$ $a - b \in S$ [by def. of kernel]

$\Rightarrow$ $a - b = 0$ [$\because$ $S = (0)$]

$\Rightarrow$ $a = b$.

$\therefore$ ϕ is one-one. Hence ϕ is an isomorphism of R into R'.

24 Ring of Real Quaternions

The quaternions of Hamilton are the first known example of a strictly skew field. Let the set H be $R \times R \times R \times R$. Then $\{R \times R \times R \times R, +\}$ is a group under addition by components, the direct product of R under addition with itself four times. This

defines the operation of addition on H. Let $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ and $k = (0, 0, 0, 1)$ be the elements of H. Also let $a_1 = (a_1, 0, 0, 0)$, $a_{2i} = (0, a_2, 0, 0), a_{3j} = (0, 0, a_3, 0)$ and $a_{4k} = (0, 0, 0, a_4)$.

By the definition of addition, we have

$$(a_1, a_2, a_3, a_4) = a_1 + a_2 i + a_3 j + a_4 k$$

$$\therefore \quad (a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k)$$
$$= (a_1 + b_1) + (a_2 + b_2) i + (a_3 + b_3) j + (a_4 + b_4) k.$$

Further to define multiplication on H, we first define

$$1a = a1 = a \text{ for } a \in H,$$
$$i^2 = j^2 = k^2 = -1,$$

and $ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j$.

(**Note:** Consider the sequence i, j, k. The product from left to right of two adjacent elements is the next one to the right. The product from right to left of two adjacent elements is the negative of the next one to the left.)

We now define the product so as to make the distributive laws hold as

$$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k)$$
$$= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3) i$$
$$+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1) k.$$

The multiplication here is associative but not commutative as $ij = k$ and $ji = -k$. Thus H is definitely not a field. For the existence of multiplicative inverses, let $a = a_1 + a_2 i + a_3 j + a_4 k$, with not all $a_i = 0$.

$$\therefore \quad (a_1 + a_2 i + a_3 j + a_4 k)(a_1 - a_2 i - a_3 j - a_4 k) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

If $|a|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and $\bar{a} = a_1 - a_2 i - a_3 j - a_4 k$, then

$$\frac{\bar{a}}{|a|^2} = \frac{a_1}{|a|^2} - \left(\frac{a_2}{|a|^2}\right) i - \left(\frac{a_3}{|a|^2}\right) j - \left(\frac{a_4}{|a|^2}\right) k$$

is a multiplicative inverse for a.

This proves the following theorem.

Theorem: *The quaternions H form a strictly skew field under addition and multiplication.*

Comprehensive Exercise 3

1. Show that every homomorphic image of a commutative ring is commutative.
2. If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R' prove that $\phi(1)$ is the unity element of R'.

3. If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that kernel of ϕ *i.e.*, $I(\phi) \neq R$, then prove that $\phi(1)$ is the unity element of R'.

4. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.

Or

Show that a field has no proper homomorphic image.

Objective Type Questions

Multiple Choice Questions

Indicate the correct answer for each question by writing the corresponding letter from (a), (b), (c) *and* (d).

1. Let R be the ring of all 2×2 matrices having elements as integers. The subset S of all matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ with a and b integers forms a

(a) subring of R (b) right ideal in R
(c) left ideal in R (d) ideal in R

2. The necessary and sufficient conditions for a non-empty subset S of a ring R to be a subring of R are

(a) $a \in S, b \in S \Rightarrow a + b \in S$ and $ab \in S$
(b) $a \in S, b \in S \Rightarrow a - b \in S$ and $ab \in S$
(c) $a \in S, b \in S \Rightarrow a - b \in S$ and $\frac{a}{b} \in S$
(d) none of these

3. The necessary and sufficient conditions for a non-empty subset K of a field F to be a subfield of F are

(a) $a \in K, b \in K \Rightarrow a - b \in K$ and $ab \in K$
(b) $a \in K, b \in K \Rightarrow a + b \in K$ and $ab \in K$
(c) $a \in K, b \in K \Rightarrow a - b \in K$ and $ab^{-1} \in K$
(d) none of these

4. An additive subgroup S of a ring R is said to be left ideal of R if

(a) $a \in S, r \in R \Rightarrow ra \in S$
(b) $a \in S, r \in R \Rightarrow ar \in S$
(c) $a \in S, r \in R \Rightarrow r - a \in S$
(d) $a \in S, r \in R \Rightarrow a - r \in S$

5. Every ring R always possesses two improper ideals : one R itself and the other consisting of 0 only. These are respectively known as
 (a) the null ideal and the unit ideal
 (b) the principal ideal and the null ideal
 (c) the unit ideal and the null ideal
 (d) none of these

Fill in the Blank(s)

Fill in the blanks "……", so that the following statements are complete and correct.

1. The intersection of two subrings is always a …… .
2. A non-empty subset K of a field F is a subfield of K if and only if
 (i) $a \in K, b \in K \Rightarrow a - b \in K$ and
 (ii) $a \in K, 0 \neq b \in K \Rightarrow \ldots\ldots \in K$.
3. If S_1 and S_2 are two subrings of a ring R, then $S_1 \cup S_2$ is a subring of R if and only if $S_1 \subseteq S_2$ or $S_2 \subseteq \ldots\ldots$
4. A non-empty subset S of a ring R is a subring of R if and only if
 (i) $a \in S, b \in S \Rightarrow a - b \in S$ and
 (ii) $a \in S, b \in S \Rightarrow \ldots\ldots$
5. A ring having no proper ideals is called a …… .
6. If R is any ring, then $\{0\}$ and R itself are always subrings of R. These are known as …… subrings of R.
7. Every ring with unity has at least two principal ideals, namely, …… and …… .

True or False

Write 'T' for true and 'F' for false statement.

1. The set of all positive rational numbers is a subring of the ring of all rational numbers.
2. A subring of any field is a field. **(Meerut 2003)**
3. The field of rational numbers is a subfield of the field of real numbers.
4. The ring of integers is a subfield of the field of rational numbers.
5. The union of two subrings is always a subring.
6. If m is a given positive integer, then
 $$S = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$$
 is a subring of the ring of integers.
7. If $S = \{0, 2, 4, 6, 8, \ldots\ldots\}$, then S is a subring of the ring of integers.

Answers

Multiple Choice Questions

1. (a) **2.** (b) **3.** (c) **4.** (a) **5.** (c)

Fill in the Blank(s)

1. subring **2.** ab^{-1} **3.** S_1 **4.** $ab \in S$
5. simple ring **6.** improper **7.** (0), (1)

True or False

1. *F* **2.** *F* **3.** *T* **4.** *F* **5.** *F*
6. *T* **7.** *F*

□



1 Polynomial Rings

While studying algebra in high school classes we are introduced with polynomials. We know that expressions of the type $3x^2 - 4x + 5, x + 7,$ $9x^3 - \frac{2}{3}x^2 + 4x + 5$ etc. are called polynomials in the *indeterminate* x. In place of x we can use other letters like y, z etc. to denote these polynomials. Now we shall define polynomials over an arbitrary ring.

Definition: *Let R be an arbitrary ring and let x, called an* **indeterminate**, *be any symbol not an element of R. By a polynomial in x over R is meant an expression of the form*

$$f(x) = a_0 x^0 + a_1 x + a_2 x^2 + \ldots\ldots$$

where $a_0, a_1, a_2, \ldots$, are elements of R and only a finite number of them are not equal to 0, the zero element of R.

Here x is an indeterminate. We could have used any other letter, say, y in place of x. Also $a_0 x^0, a_1 x, a_2 x^2$ etc. are called terms of the polynomial and a_0, a_1, a_2 etc. are called coefficients of these terms. All these coefficients are elements of R. The

number of terms in the polynomial $f(x)$ will be infinite but except a finite number of terms, the coefficients of all the remaining terms will be equal to 0, the zero element of the ring. The symbol '+' connecting various terms in $f(x)$ has no connection with the addition of the ring. This symbol has been used here only to connect different terms. Also x is not an element of R. The powers of x are nothing to do with the powers of an element of R. The different powers of x only tell us the ordered place of different coefficients. There is no harm if we represent this polynomial $f(x)$ by the infinite ordered set $(a_0, a_1, a_2, \ldots\ldots)$, where $a_0, a_1, a_2, \ldots\ldots$ are elements of R and only a finite number of them are not equal to zero. Since from high school classes we represent a polynomial with an indeterminate x, therefore we have preferred this way to represent polynomials.

Remark: The polynomial $a_0 x^0 + a_1 x + a_2 x^2 + \ldots\ldots$ over a ring R can also be written as

$$a_0 + a_1 x + a_2 x^2 + \ldots$$

2 Set of all Polynomials over a Ring

Let R be an arbitrary ring and x an indeterminate. The set of all polynomials $f(x)$,

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 x^0 + a_1 x + a_2 x^2 + \ldots$$

where the a's are elements of the ring R and only a finite number of them are not equal to zero, is called $R[x]$.

We shall make a ring out of $R[x]$. Then $R[x]$ will be called the ring of all polynomials over the ring R. For this we shall define **equality, addition** and **multiplication** of two elements of $R[x]$.

Definitions:

Suppose R is an arbitrary ring and $f(x) = a_0 x^0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$ *and* $g(x) = b_0 x^0 + b_1 x + b_2 x^2 + b_3 x^3 + \ldots$ *are any elements of* $R[x]$. *Then*

(a) **Equality of Polynomials:** $f(x) = g(x)$ *if and only if* $a_n = b_n$ $\forall$ *non-negative integer n. Thus two polynomials are equal iff their corresponding coefficients are equal.*

(b) **Addition of Polynomials:** $f(x) + g(x) = c_0 x^0 + c_1 x + c_2 x^2 + c_3 x^3 + \ldots$

where $c_n = a_n + b_n$ *for every non-negative integer n. Thus in order to add two polynomials we should add the coefficients of like powers of x.*

Since $c_n \in R$ and only a finite number of c's can be not equal to zero, therefore $f(x) + g(x)$ is an element of $R[x]$. Thus $R[x]$ is closed with respect to addition of polynomials as defined above.

(c) **Multiplication of Polynomials:**

$$f(x)\, g(x) = d_0 x^0 + d_1 x + d_2 x^2 + d_3 x^3 + \ldots$$

where $d_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0$

for every non-negative integer n.

We can write $d_n = \sum_{i+j=n} a_i\, b_j$, where by this summation we mean the sum of all the products of the type $a_i\, b_j$ with i and j non-negative integers whose sum is n.

Since $d_n \in R$ and only a finite number of d's can be not equal to zero, therefore $f(x)\, g(x)$ is an element of $R[x]$. Thus $R[x]$ is closed with respect to multiplication of polynomials as defined above.

We have $d_0 = a_0 b_0, d_1 = a_0 b_1 + a_1 b_0, d_2 = a_0 b_2 + a_1 b_1 + a_2 b_0,$

$d_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$ and so on.

Therefore in order to multiply two polynomials $f(x)$ and $g(x)$, we should first write

$$f(x)\, g(x) = (a_0 x^0 + a_1 x + a_2 x^2 + \ldots)(b_0 x^0 + b_1 x + b_2 x^2 + \ldots).$$

Now we should multiply different powers of the indeterminate x and using the relation $x^i\, x^j = x^{i+j}$ we should collect coefficients of different powers of x.

3 Zero Polynomial

Definition: *The polynomial*

$$f(x) = \Sigma\, a_n x^n = a_0 x^0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$$

in which all the coefficients $a_0, a_1, a_2, \ldots\ldots$ *are equal to* 0 *is called the zero polynomial over the ring R.*

4 Degree of a Polynomial

Definition: *Let* $f(x) = a_0 x^0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_n x^n + \ldots$

be a polynomial over an arbitrary ring R. We say that n is the degree of the polynomial $f(x)$ *if and only if* $a_n \neq 0$ *and* $a_m = 0$ *for all* $m > n$. We shall write *deg* $f(x)$ to denote the degree of $f(x)$. Thus the degree of $f(x)$ is the largest non-negative integer i for which the i^{th} coefficient of $f(x)$ is not 0. If in the polynomial $f(x)$, a_0 (*i.e.*, the coefficient of x^0) is not 0 and all the other coefficients are 0, then according to our definition, the degree of $f(x)$ will be zero. Also according to our definition, if there is no non-zero coefficient in $f(x)$, then its degree will remain undefined. Thus we do not define the degree of the zero polynomial. Also it is obvious that every non-zero polynomial will possess a unique degree.

Note: If $f(x) = a_0 x^0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$ is a polynomial of degree n *i.e.*, if $a_n \neq 0$ and $a_m = 0$ for all $m > n$, then it is convenient to write

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 x^0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.$$

It will remain understood that all the terms in $f(x)$ which follow the term $a_n x^n$, have zero coefficients. Also we shall call $a_n x^n$ as the **leading term** and a_n as the **leading coefficient** of the polynomial. The term $a_0 x^0$ is called the **constant term** and a_0 is called the zeroth coefficient of $f(x)$.

For example $f(x) = 2x^0 + 3x - 4x^2 + 4x^3 - 8x^4$ is a polynomial of degree 4 over the ring of integers. Here -8 is the leading coefficient and 2 is the zeroth coefficient. The coefficients of all terms which contain powers of x greater than 4 will be regarded as zero. Similarly $g(x) = 3x^0$ is a polynomial of degree zero over the ring of integers. In this polynomial the coefficients of $x, x^2, x^3, \ldots$ are all equal to zero. The zero polynomial over an arbitrary ring R will be represented by $0x^0$.

5 Set of Constant Polynomials over a Ring

Definition: *Let R be an arbitrary ring and R [x] the set of all polynomials over R. Let R′ denote the set of all polynomials over R whose coefficients are all zero except for the constant term, which may be either zero or non-zero. That is,*

$$R' = \{ax^0 : a \in R\}.$$

Then R′ will be called as the set of constant polynomials in R [x].

Thus all the polynomials of degree 0 as well as the zero polynomial will be called as constant polynomials.

Illustrative Examples

Example 1: *Add and multiply the following polynomials over the ring of integers:*

$$f(x) = 2x^0 + 5x + 3x^2 - 4x^3,\ g(x) = 3x^0 + 4x - x^3 + 5x^4.$$

Solution: By our definition of the sum of two polynomials, we have

$$f(x) + g(x) = (2+3)x^0 + (5+4)x + (3+0)x^2 + (-4-1)x^3 + (0+5)x^4$$
$$= 5x^0 + 9x + 3x^2 - 5x^3 + 5x^4.$$

Also
$$f(x)\, g(x) = (2x^0 + 5x + 3x^2 - 4x^3)(3x^0 + 4x - x^3 + 5x^4)$$
$$= 6x^0 + (8+15)x + (20+9)x^2 + (-2+12-12)x^3 + (10-5-16)x^4 + (25-3)x^5 + (15+4)x^6 - 20x^7$$
$$= 6x^0 + 23x + 29x^2 - 2x^3 - 11x^4 + 22x^5 + 19x^6 - 20x^7.$$

Example 2: *Add and multiply the following polynomials over the ring* $(\mathbf{I}_6, +_6, \times_6)$*:*

$$f(x) = 2x^0 + 5x + 3x^2,\ g(x) = 1x^0 + 4x + 2x^3.$$

Solution: $f(x) + g(x) = (2 +_6 1)\,x^0 + (5 +_6 4)\,x + (3 +_6 0)\,x^2 + (0 +_6 2)\,x^3$

$= 3x^0 + 3x + 3x^2 + 2x^3.$

Also $f(x)\,g(x) = (2x^0 + 5x + 3x^2)(1x^0 + 4x + 2x^3)$

$= (2 \times_6 1)\,x^0 + [(2 \times_6 4) +_6 (5 \times_6 1)]\,x$

$+ [(5 \times_6 4) +_6 (3 \times_6 1)]\,x^2 + [(2 \times_6 2) +_6 (3 \times_6 4)]\,x^3$

$+ (5 \times_6 2)\,x^4 + (3 \times_6 2)\,x^5$

$= 2x^0 + (2 +_6 5)\,x + (2 +_6 3)\,x^2 + (4 +_6 0)\,x^3$

$+ 4x^4 + 0x^5$

$= 2x^0 + 1x + 5x^2 + 4x^3 + 4x^4.$

Note: Here degree of $f(x) = 2$, degree of $g(x) = 3$ and degree of $f(x)\,g(x) = 4$. The point to note is that degree $f(x)\,g(x)$ may be less than the sum of the degrees of $f(x)$ and $g(x)$.

Example 3: *Add and multiply the following polynomials over the ring* $(\mathbf{I}_5, +_5, \times_5)$:

$f(x) = 3 + 4x + 2x^2,\ g(x) = 1 + 3x + 4x^2 + 2x^3.$

Solution : $f(x) + g(x) = 4 + 2x + x^2 + 2x^3,$

$f(x)\,g(x) = 3 + 3x + x^2 + 3x^3 + x^4 + 4x^5.$

6 Degree of the Sum and the Product of Two Polynomials

Theorem: *Let* $f(x)$ *and* $g(x)$ *be two non-zero polynomials over an arbitrary ring* R. *Then*

(i) $\deg[f(x) + g(x)] \le Max[\deg f(x), \deg g(x)]$, *if* $f(x) + g(x) \neq 0$.

(ii) $\deg[f(x)\,g(x)] \le \deg f(x) + \deg g(x)$, *if* $f(x)\,g(x) \neq 0$.

Proof: Let $f(x) = a_0 x^0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,\ a_n \neq 0$

and $g(x) = b_0 x^0 + b_1 x + b_2 x^2 + \ldots + b_m x^m,\ b_m \neq 0$

be two elements of $R[x]$.

Here $\deg f(x) = n$ and $\deg g(x) = m$.

From our definition of the sum of two polynomials, it is obvious that if

$f(x) + g(x) \neq 0$, then

$$\deg[f(x)+g(x)] = \begin{cases} \max(n,m) & \text{if } n \neq m \\ n \text{ if } n = m \text{ and } a_n + b_m \neq 0 \\ < n \text{ if } n = m \text{ and } a_n + b_m = 0. \end{cases}$$

Again $f(x)\,g(x) = (a_0 b_0)x^0 + (a_0 b_1 + a_1 b_0)\,x + \ldots + a_n b_m x^{n+m}.$

Suppose $f(x)\,g(x) \neq 0$. Then $f(x)\,g(x)$ has a unique degree.

If $a_n b_m \neq 0$, then deg $[f(x)\ g(x)] = n + m = \deg f(x) + \deg g(x)$.

Also if $a_n b_m = 0$, then deg $[f(x)\ g(x)] < n + m$.

Corollary 1: *Suppose D is an integral domain and $f(x)$, $g(x)$ are two non-zero elements of $D[x]$. Then*

$$deg\,[f(x)\ g(x)] = deg\ f(x) + deg\ g(x).$$ **(Gorakhpur 2014)**

Proof: Since $a_n \neq 0$, $b_m \neq 0$, therefore $a_n\ b_m \neq 0$ because in an integral domain the product of two non-zero elements cannot be zero. Hence deg$[f(x)\ g(x)] = m + n$.

Corollary 2: *If F is a field and $f(x)$, $g(x)$ are two non-zero elements of $F[x]$, then*

$$deg\,[f(x)\ g(x)] = deg\ f(x) + deg\ g(x).$$

Proof: Since a field is also free from zero divisors, therefore $a_n b_m \neq 0$ when $a_n \neq 0$ and $b_m \neq 0$. Hence the result.

7 Ring of Polynomials

Theorem: *The set $R[x]$ of all polynomials over an arbitrary ring R is a ring with respect to addition and multiplication of polynomials.*

Proof: Let $f(x), g(x) \in R[x]$. Then $f(x) + g(x)$ and $f(x)\ g(x)$ are also polynomials over R. Therefore $R[x]$ is closed with respect to addition and multiplication of polynomials.

Now let $f(x) = \Sigma\, a_i x^i = a_0 x^0 + a_1 x + a_2 x^2 + \ldots,$

$g(x) = b_0 x^0 + b_1 x + b_2 x^2 + \ldots,$

$h(x) = c_0 x^0 + c_1 x + c_2 x^2 + \ldots$ be any arbitrary elements of $R[x]$.

Commutativity of addition: We have

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) x^0 + (a_1 + b_1) x + (a_2 + b_2) x^2 + \ldots \\ &= (b_0 + a_0) x^0 + (b_1 + a_1) x + (b_2 + a_2) x^2 + \ldots \\ &= g(x) + f(x). \end{aligned}$$

Associativity of addition: We have

$$\begin{aligned} [f(x) + g(x)] + h(x) &= \Sigma\, (a_i + b_i) x^i + \Sigma\, c_i x^i \\ &= \Sigma\, [(a_i + b_i) + c_i]\, x^i = \Sigma\, [a_i + (b_i + c_i)]\, x^i \\ &= \Sigma\, a_i x^i + \Sigma\, (b_i + c_i) x^i = f(x) + [g(x) + h(x)]. \end{aligned}$$

Existence of additive identity: Let $0(x)$ be the zero polynomial over R *i.e.*,

$$0(x) = 0x^0 + 0x + 0x^2 + \ldots$$

Then $$\begin{aligned} f(x) + 0(x) &= (a_0 + 0) x^0 + (a_1 + 0) x + (a_2 + 0) x^2 + \ldots \\ &= a_0 x^0 + a_1 x + a_2 x^2 + \ldots = f(x). \end{aligned}$$

$\therefore$ the zero polynomial $0(x)$ is the additive identity.

Existence of additive inverse: Let $-f(x)$ be the polynomial over R defined as

$$-f(x) = (-a_0)x^0 + (-a_1)x + (-a_2)x^2 + \ldots$$

Then
$$-f(x) + f(x) = (-a_0 + a_0)x^0 + (-a_1 + a_1)x + (-a_2 + a_2)x^2 + \ldots$$
$$= 0x^0 + 0x + 0x^2 + \ldots = 0(x)$$
$$= \text{the additive identity.}$$

$\therefore$ each member of $R[x]$ possesses additive inverse.

Associativity of Multiplication: We have

$$f(x)\,g(x) = (a_0x^0 + a_1x + a_2x^2 + \ldots)(b_0x^0 + b_1x + b_2x^2 + \ldots)$$
$$= d_0x^0 + d_1x + d_2x^2 + \ldots + d_lx^l + \ldots,$$
$$\text{where } d_l = \sum_{i+j=l} a_ib_j .$$

Now
$$[f(x)\,g(x)]h(x) = (d_0x^0 + d_1x + d_2x^2 + \ldots)(c_0x^0 + c_1x + c_2x^2 + \ldots)$$
$$= e_0x^0 + e_1x + e_2x^2 + \ldots + e_nx^n + \ldots,$$
$$\text{where } e_n = \text{the coeff. of } x^n \text{ in } [f(x)\,g(x)]\,h(x)$$
$$= \sum_{l+k=n} d_lc_k = \sum_{l+k=n} \left[\left(\sum_{i+j=l} a_ib_j\right)c_k\right]$$
$$= \sum_{i+j+k=n} a_ib_jc_k.$$

Similarly we can show that the coeff. of x^n in $f(x)[g(x)\,h(x)]$
$$= \sum_{i+j+k=n} a_ib_jc_k.$$

Thus $[f(x)\,g(x)]\,h(x) = f(x)[g(x)\,h(x)]$ since corresponding coefficients in these two polynomials are equal.

Distributivity of Multiplication with respect to addition: We have

$$f(x)[g(x) + h(x)] = (a_0x^0 + a_1x + a_2x^2 + \ldots)$$
$$[(b_0 + c_0)x^0 + (b_1 + c_1)x + (b_2 + c_2)x^2 + \ldots]$$

If n is any non-negative integer, then the coefficient of x^n in $f(x)[g(x) + h(x)]$

$$= \sum_{i+j=n} a_i(b_j + c_j) = \sum_{i+j=n} (a_ib_j + a_ic_j)$$
$$= \sum_{i+j=n} a_ib_j + \sum_{i+j=n} a_ic_j$$
$$= \text{Coeff. of } x^n \text{ in } f(x)\,g(x) + \text{coeff. of } x^n \text{ in } f(x)\,h(x)$$
$$= \text{Coeff. of } x^n \text{ in } [f(x)\,g(x) + f(x)\,h(x)].$$

$\therefore$ $f(x)[g(x) + h(x)] = f(x)\,g(x) + f(x)\,h(x)$.

Similarly we can prove the right distributive law.

Hence $R[x]$ is a ring. This is called the ring of all polynomials over R. The zero element of this ring is the zero polynomial

$$0x^0 + 0x + 0x^2 + 0x^3 + \ldots$$

8 R as a Subset of $R[x]$ or Embedding of R into $R[x]$

Theorem: *If R is an arbitrary ring and R' is the set of constant polynomials in $R[x]$, then R' is isomorphic to R.*

Proof: We have

$$R' = \{ax^0 + 0x + 0x^2 + 0x^3 + \ldots. \text{ such that } a \in R\}.$$

Let $\phi : R \to R'$ such that

$$\phi(a) = ax^0 + 0x + 0x^2 + 0x^3 + \ldots. \quad \forall \quad a \in R.$$

ϕ is one-one since

$$\phi(a) = \phi(b) \quad \Rightarrow \quad ax^0 + 0x + 0x^2 + \ldots. = bx^0 + 0x + 0x^2 + \ldots$$

$$\Rightarrow \qquad a = b.$$

Also ϕ is obviously onto R'.

Again
$$\phi(a + b) = (a + b)\, x^0 + 0x + 0x^2 + 0x^3 + \ldots.$$
$$= [ax^0 + 0x + 0x^2 + \ldots.] + [bx^0 + 0x + 0x^2 + \ldots]$$
$$= \phi(a) + \phi(b).$$

Also
$$\phi(ab) = abx^0 + 0x + 0x^2 + 0x^3 + \ldots.$$
$$= (ax^0 + 0x + 0x^2 + \ldots)\,(bx^0 + 0x + 0x^2 + \ldots.) = \phi(a)\,\phi(b).$$

$\therefore$ ϕ is an isomorphism of R onto R'. Hence $R \cong R'$.

Since R is isomorphic to R', therefore in $R[x]$ we can identify R' by R *i.e.,* all the constant polynomials in $R[x]$ can be replaced by the corresponding elements of R. This replacement will not affect the addition and multiplication of polynomials.

Hence in future we shall write 0 in place of the zero polynomial. If $ax^0 + 0x + 0x^2 + \ldots.$ is any constant polynomial in $R[x]$, then we shall simply write a in place of this polynomial.

Also in place of $a_0 x^0 + a_1 x + a_2 x^2 + \ldots$ we shall write $a_0 + a_1 x + a_2 x^2 + \ldots.$. If we are to multiply $f(x)$ by a constant polynomial $ax^0 + 0x + 0x^2 + \ldots$, then we shall write $af(x)$ in place of $(ax^0 + 0x + \ldots.)\, f(x)$.

9 Polynomials over an Integral Domain

Theorem 1: *If D is an integral domain, then the polynomial ring $D[x]$ is also an integral domain.* **(Gorakhpur 2012, 15)**

Proof: Let D be a commutative ring without zero divisors and with unity element 1. As proved in article 7, $D[x]$ is also a ring. To prove that $D[x]$ is an integral domain we should prove that (i) $D[x]$ is commutative, (ii) is without zero divisors and (iii) possesses the unity element.

***D* [*x*] is commutative:** Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots$$

and $g(x) = b_0 + b_1 x + b_2 x^2 + \ldots\ldots$ be any two elements of $D[x]$.

If n is any non-negative integer, then the coefficient of x^n in $f(x)\, g(x)$ is

$$= \sum_{i+j=n} a_i\, b_j = \sum_{i+j=n} b_j\, a_i, \text{ since } D \text{ is commutative}$$

$$= \text{coefficient of } x^n \text{ in } g(x)\, f(x).$$

$\therefore$ $f(x)\, g(x) = g(x)\, f(x)$.

Hence $D[x]$ is a commutative ring.

If 1 is the unity element of D, then the constant polynomial

$$1 + 0x + 0x^2 + 0x^3 + \ldots$$

is the unity element of $D[x]$. We have

$$[a_0 + a_1 x + a_2 x^2 + \ldots][1 + 0x + 0x^2 + 0x^3 + \ldots]$$

$$= (a_0 1) + (a_1 1)\, x + (a_2 1)\, x^2 + \ldots = a_0 + a_1 x + a_2 x^2 + \ldots$$

$\therefore$ the polynomial $1 + 0x + 0x^2 + \ldots$ or simply 1 is the unity element of $D[x]$.

***D* [*x*] is without zero divisors:** Let

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m,\ a_m \neq 0$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n,\ b_n \neq 0$$

be two non-zero elements of $D[x]$.

Then $f(x)\, g(x)$ cannot be a zero polynomial *i.e.*, the zero element of $D[x]$. The reason is that at least one coefficient of $f(x)\, g(x)$ namely $a_m b_n$ of x^{m+n} is $\neq 0$ because a_m, b_n are non-zero elements of D and D is without zero divisors.

Hence $D[x]$ is an integral domain.

Theorem 2: *If R is an integral domain with unity element, then any unit in $R[x]$ must already be a unit in R.* **(Gorakhpur 2013)**

Proof: If R is an integral domain with unity element 1, then $R[x]$ is also an integral domain with unity element. Further the constant polynomial 1 is the unity element of $R[x]$. Let $f(x)$ be a unit in $R[x]$ *i.e.*, let $f(x)$ be an inversible element of $R[x]$. Let $g(x)$ be the inverse of $f(x)$ in $R[x]$. Then

$$f(x)\, g(x) = 1$$

$\Rightarrow$ $\deg[f(x)\, g(x)] = 0$

$[\because$ degree of the constant polynomial 1 is 0$]$

$\Rightarrow$ $\deg f(x) + \deg g(x) = 0$

$\Rightarrow$ $\deg f(x) = 0, \deg g(x) = 0$

$\Rightarrow$ both $f(x)$ and $g(x)$ are constant polynomials in $R[x]$.

Let $f(x) = a \in R$ and $g(x) = b \in R$. Then $ab = 1 \Rightarrow a$ is a unit in R. Thus any unit in $R[x]$ must already be a unit in R.

Note: If $a \in R$ is a unit in R, then $a \in R[x]$ is also a unit in $R[x]$. If b is the inverse of a in R, then the constant polynomial b is the inverse of a in $R[x]$.

10 Polynomials over a Field

Theorem 1: *If F is a field, then the set $F[x]$ of all polynomials over F is an integral domain.*

(Gorakhpur 2011)

Proof: Every field is an integral domain. So give the same proof as we have given in article 7 and then in article 9.

We shall call the set $F[x]$ as the polynomial domain over the field F.

Theorem 2: *The polynomial domain $F[x]$ over a field F is not a field.*

Proof: In order to show that $F[x]$ is not a field, we should show that there exists a non-zero element of $F[x]$ which has no multiplicative inverse. Let $f(x)$ be any member of $F[x]$ such that $\deg f(x)$ is greater than zero. The inverse of $f(x)$ cannot be the zero polynomial because the product of $f(x)$ and the zero polynomial will be equal to the zero polynomial and not equal to the unity element of $F[x]$ which is the polynomial $1 + 0x + 0x^2 + \ldots$. Suppose now $g(x)$ is any non-zero polynomial.Then F being a field, we have

$$\deg [f(x)\, g(x)] = \deg f(x) + \deg g(x) > 0$$

because $\deg f(x) > 0$ and $\deg g(x) \geq 0$.

The degree of the unity element of $F[x]$ is 0. Hence $f(x)\, g(x)$ cannot be equal to the unity element of $F[x]$. Thus $f(x)$ does not possess multiplicative inverse.

$\therefore$ $F[x]$ is not a field.

Important: The only inversible elements of $F[x]$ are constant polynomials excluding the zero polynomial. No member of $F[x]$ whose degree is greater than 0 is inversible.

Illustrative Examples

Example 4: *Show that if a ring R has no zero divisors, then the ring $R[x]$ has also no zero divisors.*

Solution: It is given that a ring R has no zero divisors and we have to show that the ring $R[x]$ has also no zero divisors.

Let $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_m x^m, a_m \neq 0$

and $g(x) = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n, b_n \neq 0$

be two non-zero elements of $R[x]$.

Then $f(x)\ g(x)$ cannot be the zero polynomial *i.e.,* the zero element of $R[x]$. The reason is that at least one coefficient of $f(x)\ g(x)$ namely $a_m b_n$ of x^{m+n} is $\neq 0$ because a_m, b_n are non-zero elements of R and R is without zero divisors.

Thus in $R[x]$ the product of no two non-zero elements can be the zero element. Hence the ring $R[x]$ has no zero divisors.

Example 5: *Consider the following polynomials over the ring* $(\mathbf{I}_8, +_8, \times_8)$:

$$f(x) = 2 + 6x + 4x^2,\ g(x) = 2x + 4x^2,\ h(x) = 2 + 4x$$

and find *(i)* $deg[f(x) + g(x)]$

(ii) $deg[f(x)\ g(x)]$

(iii) $deg[h(x)\ h(x)]$.

Solution: **(i)** We have

$$\begin{aligned} f(x) + g(x) &= (2 + 6x + 4x^2) + (0 + 2x + 4x^2) \\ &= (2 +_8 0) + (6 +_8 2)\ x + (4 +_8 4)\ x^2 \\ &= 2 + 0x + 0x^2 = 2. \end{aligned}$$

Thus $f(x) + g(x)$ is a non-zero constant polynomial and so

$$\deg[f(x) + g(x)] = 0.$$

(ii) We have $f(x)\ g(x) = (2 + 6x + 4x^2)(2x + 4x^2)$

$$\begin{aligned} &= (2 \times_8 2)\ x + [(2 \times_8 4) +_8 (6 \times_8 2)]\ x^2 \\ &\qquad + [(6 \times_8 4) +_8 (4 \times_8 2)]\ x^3 + (4 \times_8 4)\ x^4 \\ &= 4x + (0 +_8 4)\ x^2 + (0 +_8 0)\ x^3 + 0x^4 \\ &= 4x + 4x^2 + 0x^3 + 0x^4 = 4x + 4x^2 \end{aligned}$$

$\therefore$ $\deg[f(x)\ g(x)] = 2.$

(iii) We have $h(x)\ h(x) = (2 + 4x)(2 + 4x)$

$$\begin{aligned} &= (2 \times_8 2) + [(2 \times_8 4) +_8 (4 \times_8 2)]\ x + (4 \times_8 4)\ x^2 \\ &= 4 + (0 +_8 0)\ x + 0x^2 = 4 + 0x + 0x^2 = 4. \end{aligned}$$

Thus $h(x)\ h(x)$ is a non-zero constant polynomial and so $\deg[h(x)\ h(x)] = 0$.

11 Ring of Polynomials in n Variables over an Integral Domain

Definition: *Let R be an integral domain. Then the ring of polynomials in the n-variables* $x_1, \ldots, x_n$ *over R is denoted by* $R[x_1, \ldots, x_n]$ *and is defined as follows :*

Let $R_1 = R[x_1]$, *the polynomial ring in* x_1 *over* R,

$R_2 = R_1[x_2]$, *the polynomial ring in* x_2 *over* R_1,

$R_3 = R_2[x_3]$, *the polynomial ring in* x_3 *over* R_2,

...

...

$R_n = R_{n-1}[x_n]$, *the polynomial ring in* x_n *over* R_{n-1}.

Then R_n *is called the ring of polynomials in* $x_1, \ldots, x_n$ *over R and we write* $R_n = R[x_1, \ldots, x_n]$.

Theorem 1: *If R is an integral domain, then so is* $R[x_1, \ldots, x_n]$.

Proof: If R is an integral domain then $R_1 = R[x_1]$ is also an integral domain. Now R_1 is an integral domain implies that $R_2 = R_1[x_2] = R[x_1, x_2]$ is also an integral domain. Continuing this process a finite number of times we see that $R[x_1, \ldots, x_n]$ is an integral domain.

Theorem 2: *If F is a field, then* $F[x_1, \ldots, x_n]$ *is an integral domain.*

Proof: If F is a field, then $F_1 = F[x_1]$ is an integral domain.

Now F_1 is an integral domain implies that $F_2 = F_1[x_2] = F[x_1, x_2]$ is also an integral domain. Continuing this process a finite number of times we see that $F[x_1, \ldots, x_n]$ is an integral domain.

Note: If F is a field, then $F[x_1, \ldots, x_n]$ is an integral domain.

Now we can construct the field of quotients of the integral domain $F[x_1, \ldots, x_n]$. This field is called *the field of rational functions in* $x_1, \ldots, x_n$ *over F* and is denoted by $F(x_1, \ldots, x_n)$.

12 Divisibility of Polynomials over a Field

Suppose F is a field. Then $F[x]$ is an integral domain. If $a(x) \neq 0$ and $f(x)$ are elements of $F[x]$, then $a(x)$ is a *divisor* (*or factor*) of $f(x)$ if and only if there is a polynomial $b(x)$ in $F[x]$ such that $f(x) = a(x)\, b(x)$. Symbolically we write $a(x) \mid f(x)$.

A **unit** is an element of $F[x]$ which has multiplicative inverse. All the polynomials of zero degree belonging to $F[x]$ are units of $F[x]$. Thus the non-zero elements of F are the only units of $F[x]$.

If $f(x)$ and $g(x)$ are polynomials in $F[x]$, then we call $f(x)$ and $g(x)$ *associates* if $f(x) = c\,g(x)$ for some $0 \neq c \in F$. It can be easily proved that two non-zero polynomials $f(x)$ and $g(x)$ in $F[x]$ are associates if and only if $f(x) \mid g(x)$ and $g(x) \mid f(x)$.

If $f(x)$ is any non-zero polynomial in $F[x]$, then $f(x)$ is always divisible by its associates and by all units of $F[x]$. These divisors of $f(x)$ are called its *improper divisors*. All other divisors of $f(x)$, if there are any, are called its *proper divisors*.

13 Irreducible Polynomial Over a Field

Definition : *Let F be a field and $f(x)$ be a non-zero and non-unit polynomial in $F[x]$ i.e., $f(x)$ be a polynomial of positive degree. Then $f(x)$ is said to be irreducible over F (or prime) if it has no proper divisors in $F[x]$; $f(x)$ is reducible over F if it has a proper divisor in $F[x]$.*

Thus a positive degree polynomial $f(x)$ in $F[x]$ is irreducible over F if whenever $f(x) = a(x)\,b(x)$ with $a(x), b(x) \in F[x]$ then one of $a(x)$ or $b(x)$ is a unit in $F[x]$ *i.e.*, has degree 0. Also $f(x)$ is reducible over F if and only if we can find two polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $f(x) = a(x)\,b(x)$ and none of $a(x)$ and $b(x)$ is a unit in $F[x]$ *i.e.*, has degree 0.

Irreducibility depends on the field. The polynomial $x^2 - 2$ is irreducible over the field of rational numbers while it is reducible over the field of real numbers, since $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$.

The polynomial $x^2 + 1$ is irreducible over the field of real numbers while it is reducible over the field of complex numbers since $x^2 + 1 = (x + i)(x - i)$.

14 Monic Polynomials

Definition: *Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, with $a_n \neq 0$, be a polynomial in $F[x]$ over an arbitrary field F. If the leading coefficient a_n of $f(x)$ is equal to 1, the unity element of F, then the polynomial $f(x)$ will be called monic.*

The polynomial $2x - 3x^3$ over the field of real numbers is not monic since its leading coefficient is -3. But the polynomial $x^3 - 3x + 4$ over the field of real numbers is monic since its leading coefficient is 1.

15 Greatest Common Divisor of Two Polynomials over a Field

Definition: *Suppose F is any field. Let $f(x)$ and $g(x)$ be two elements of $F[x]$. A greatest common divisor of $f(x)$ and $g(x)$ is a non-zero polynomial $d(x)$ such that*

(i) $d(x) \mid f(x)$ *and* $d(x) \mid g(x)$

(ii) *If* $c(x)$ *is a polynomial such that* $c(x) \mid f(x)$ *and* $c(x) \mid g(x)$ *then* $c(x) \mid d(x)$.

Relatively prime polynomials: *Two polynomials $f(x)$ and $g(x) \in F[x]$ are said to be relatively prime if their greatest common divisor is 1, the unity element of F.*

16 Division Algorithm for Polynomials over a Field

Theorem: *Let $f(x), g(x) \neq 0$ be any two polynomials of the polynomial domain $F[x]$, over the field F. Then there exist uniquely two polynomials $q(x)$ and $r(x)$ in $F[x]$ such that*

$$f(x) = q(x)\ g(x) + r(x) \quad \text{where either } r(x) = 0 \text{ or deg } r(x) < \text{deg } g(x).$$

(Gorakhpur 2011, 14)

Proof: Suppose

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m,\ a_m \neq 0$$

and

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n,\ b_n \neq 0.$$

If degree m of $f(x)$ is smaller than the degree n of $g(x)$ or if $f(x) = 0$, then we have nothing to prove . Because we can always write $f(x) = 0 \cdot g(x) + f(x)$. So in this case $q(x) = 0$, $r(x) = f(x)$ and we have either $f(x) = 0$ or deg $f(x) <$ deg $g(x)$.

Now let us assume that $m \geq n$. In this case we shall prove the theorem by induction on m *i.e.*, degree of $f(x)$.

If $m = 0$, then $m \geq n \Rightarrow n = 0$. Therefore $f(x)$ and $g(x)$ are both non-zero constant polynomials, $f(x) = a_0, a_0 \neq 0$, and $g(x) = b_0, b_0 \neq 0$.

We have in this case

$$f(x) = a_0 = (a_0\ b_0^{-1})\ b_0 + 0 = (a_0\ b_0^{-1})\ g(x) + 0.$$

Thus the theorem is true when $m = 0$ or when the degree of $f(x)$ is less than 1.

We shall now assume that the theorem is true when $f(x)$ is a polynomial of degree less than m and then we shall show that it is also true if $f(x)$ is of degree m and then the proof will be complete by induction.

Let

$$f_1(x) = f(x) - (a_m\ b_n^{-1})\ x^{m-n}\ g(x) \qquad \ldots(1)$$

Obviously deg $f_1(x) < m$. Therefore by our assumed hypothesis, there exist polynomials $s(x)$ and $r(x)$ such that

$$f_1(x) = s(x)\ g(x) + r(x),$$

where

$$r(x) = 0 \quad \text{or} \quad \text{deg } r(x) < \text{deg } g(x).$$

Now putting the value of $f_1(x)$ in (1), we get

$$s(x)\ g(x) + r(x) = f(x) - (a_m\ b_n^{-1})\ x^{m-n}\ g(x)$$

or $$f(x) = [(a_m\ b_n^{-1})\ x^{m-n} + s(x)]\ g(x) + r(x).$$

If we write $q(x)$ in place of $(a_m\ b_n{}^{-1})\ x^{m-n} + s(x)$, we get

$$f(x) = q(x)\ g(x) + r(x)$$

where $r(x) = 0$ or $\deg\ r(x) < \deg\ g(x)$.

This proves the existence of polynomials $q(x)$ and $r(x)$. Now to show that $q(x)$ and $r(x)$ are unique. Let us assume that

$$f(x) = q_1(x)\ g(x) + r_1(x) = q_2(x)\ g(x) + r_2(x).$$

Then $$q_1(x)\ g(x) + r_1(x) = q_2(x)\ g(x) + r_2(x)$$

or $$[q_1(x) - q_2(x)]\ g(x) = r_2(x) - r_1(x). \qquad ...(2)$$

If $[q_1(x) - q_2(x)] \neq 0$, then $[q_1(x) - q_2(x)]\ g(x)$ cannot be equal to the zero polynomial because $g(x) \neq 0$ and $F[x]$ is without zero divisors. Also then the degree of $[q_1(x) - q_2(x)]\ g(x)$ is at least n, the degree of $g(x)$. But $r_2(x) - r_1(x)$ is either equal to the zero polynomial or else its degree is less than n because the degrees of $r_2(x)$ and $r_1(x)$ are both less than n. Hence the equality (2) among two polynomials holds only if

$$q_1(x) - q_2(x) = 0 \quad \text{and} \quad r_2(x) - r_1(x) = 0$$

i.e., only if $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$.

$\therefore$ the polynomials $q(x)$ and $r(x)$ are unique.

Definition: *In the division algorithm, the polynomial $q(x)$ is called the* **quotient** *on dividing $f(x)$ by $g(x)$ and the polynomial $r(x)$ is called the* **remainder.**

Theorem: *A polynomial domain $F[x]$ over a field F is a principal ideal ring.*

Proof: Obviously $F[x]$ is a commutative ring with unity and without zero divisors. Therefore $F[x]$ is a principal ideal ring if every ideal in $F[x]$ is a principal ideal.

Let S be an arbitrary ideal of $F[x]$. If S is the null ideal, then $S = (0)$ *i.e.*, the ideal of $F[x]$ generated by 0. Therefore S is a principal ideal, so let us suppose that S is not a null ideal. Then there exist non-zero polynomials $f(x)$ in S. Let $g(x)$ be a polynomial of lowest degree m belonging to S. We shall show that S is the principal ideal generated by $g(x)$.

Let $f(x)$ be any arbitrary member of S. By division algorithm there exist two polynomials $q(x) \in F[x]$, $r(x) \in F[x]$, such that

$$f(x) = q(x)\ g(x) + r(x), \text{where } r(x) = 0 \text{ or } \deg\ r(x) < \deg\ g(x).$$

Since S is an ideal, therefore

$$q(x) \in F[x],\ g(x) \in S \ \Rightarrow\ q(x)\ g(x) \in S.$$

Also $f(x) \in S,\ q(x)\ g(x) \in S \Rightarrow f(x) - q(x)\ g(x) \in S.$

But $f(x) - q(x)\ g(x) = r(x)$. Therefore $r(x) \in S$.

Now either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. But we have assumed that $g(x)$ is a polynomial of lowest degree belonging to S. Hence $\deg r(x)$ cannot be less than $\deg g(x)$. Therefore we must have $r(x) = 0$. Then $f(x) = q(x)\ g(x)$. Thus $g(x) \in S$ is such that $f(x) \in S \Rightarrow f(x) = q(x)\ g(x)$ for some $q(x) \in F[x]$. Therefore S is a principal ideal of $F[x]$ generated by $g(x)$. Hence $F[x]$ is a principal ideal ring.

Important: A polynomial ring over an arbitrary field is a principal ideal ring. But a polynomial ring over an arbitrary ring is not a principal ideal ring as is obvious from the following example.

Illustrative Examples

Example 6: *Show that the polynomial ring* $\mathbf{I}[x]$ *over the ring of integers is not a principal ideal ring.*

Solution: To prove this statement we shall show that the ideal $(2, x)$ of the ring $\mathbf{I}[x]$ generated by two elements 2 and x of $\mathbf{I}[x]$ is not a principal ideal. Let $(2, x)$ be a principal ideal in $\mathbf{I}[x]$. Then there will exist a non-zero element $g(x) \in \mathbf{I}[x]$ such that $(2, x) = (g(x))$.

Since $2 \in (g(x))$ and $x \in (g(x))$ therefore there will exist elements $\phi(x)$ and $\psi(x)$ belonging to $\mathbf{I}[x]$ such that

$$2 = \phi(x)\ g(x), \qquad \ldots(1)$$

$$x = \psi(x)\ g(x). \qquad \ldots(2)$$

From (1), we get $2x = [\phi(x)\ g(x)]\ x$ and from (2), we get

$$2x = 2\ \psi(x)\ g(x).$$

$\therefore \quad 2\ \psi(x)\ g(x) = x\ \phi(x)\ g(x).$ [$\because$ $\mathbf{I}[x]$ is a commutative ring]

$\therefore \quad 2\ \psi(x) = x\ \phi(x)$, since $g(x) \neq 0$, and $\mathbf{I}[x]$ is without zero divisors.

Now $2\ \psi(x) = x\ \phi(x)$ implies that the coefficients of $\phi(x)$ must be even integers. Therefore $\phi(x) = 2h(x)$ where $h(x)$ is some polynomial in $\mathbf{I}[x]$. Putting this value of $\phi(x)$ in (1) we get

$$2 = 2h(x)\ g(x) \quad \text{or} \quad 1 = h(x)\ g(x).$$

Now $1 = h(x)\ g(x) \Rightarrow 1 \in (g(x))$. Therefore each element of $\mathbf{I}[x]$ will belong to $(g(x))$. Thus we have $\mathbf{I}[x] = (g(x)) = (2, x)$. Therefore each element of $\mathbf{I}[x]$ will belong to $(2, x)$. We shall show that $1 \notin (2, x)$ and this contradiction will mean that $(2, x)$ is not a principal ideal in $\mathbf{I}[x]$.

Now $1 \in (2, x) \Rightarrow$ we can write

$$1 = 2p(x) + x\ q(x)$$

where $p(x)$ and $q(x)$ are some elements in $\mathbf{I}[x]$.

Let $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ and $q(x) = b_0 + b_1 x + b_2 x^2 + \ldots$

Then $1 = 2(a_0 + a_1 x + a_2 x^2 + \ldots) + x(b_0 + b_1 x + b_2 x^2 + \ldots)$

or $1 = 2a_0 + (2a_1 + b_0)\, x + (2a_2 + b_1)\, x^2 + \ldots$

This equality implies $1 = 2a_0$ where $a_0 \in \mathbf{I}$.

But for no integer a_0 we can have $1 = 2a_0$. Hence $1 \notin (2, x)$.

$\therefore$ $(2, x)$ is not a principal ideal in $\mathbf{I}[x]$.

17 Euclidean Algorithm for Polynomials over a Field

Theorem: *Let F be a field and $f(x)$ and $g(x)$ be any two polynomials in $F[x]$, not both of which are zero. Then $f(x)$ and $g(x)$ have a greatest common divisor $d(x)$ which can be expressed in the form*

$$d(x) = m(x)\, f(x) + n(x)\, g(x)$$

for polynomials $m(x)$ and $n(x)$ in $F[x]$. **(Gorakhpur 2010, 15)**

Proof: Consider the set

$$S = \{ s(x)\, f(x) + t(x)\, g(x) : s(x), t(x) \in F[x] \}. \quad \ldots(1)$$

We claim that S is an ideal of $F[x]$. The proof is as follows :

Let $s_1(x)\, f(x) + t_1(x)\, g(x)$ and $s_2(x)\, f(x) + t_2(x)\, g(x)$ be any two elements of S.

Then $[s_1(x)\, f(x) + t_1(x)\, g(x)] - [s_2(x)\, f(x) + t_2(x)\, g(x)]$

$$= [s_1(x) - s_2(x)]\, f(x) + [t_1(x) - t_2(x)]\, g(x) \in S,$$

since $s_1(x) - s_2(x)$ and $t_1(x) - t_2(x)$ are both members of $F[x]$.

Also if $\alpha(x)$ be any member of $F[x]$, then

$$\alpha(x)\, [s_1(x)\, f(x) + t_1(x)\, g(x)]$$

$$= [\alpha(x)\, s_1(x)]\, f(x) + [\alpha(x)\, t_1(x)]\, g(x) \in S.$$

Therefore S is an ideal of $F[x]$. Now every ideal in $F[x]$ is a principal ideal. Therefore there exists an element $d(x)$ in S such that every element in S is a multiple of $d(x)$.

Since $d(x) \in S$, therefore from (1) we see that there exist elements $m(x)$, $n(x) \in F[x]$ such that

$$d(x) = m(x)\, f(x) + n(x)\, g(x).$$

Now $F[x]$ is a ring with unity element 1.

$\therefore$ Putting $s(x) = 1$, $t(x) = 0$ in (1), we see that $f(x) \in S$. Also putting $s(x) = 0$, $t(x) = 1$ in (1), we see that $g(x) \in S$.

Now $f(x)$, $g(x)$ are elements of S. Therefore they are both multiples of $d(x)$. Hence $d(x) \mid f(x)$ and $d(x) \mid g(x)$.

Now suppose $c(x) \mid f(x)$ and $c(x) \mid g(x)$.

Then $c(x) \mid [m(x)\, f(x)]$ and $c(x) \mid [n(x)\, g(x)]$. Therefore $c(x)$ is also a divisor of

$m(x)\ f(x) + n(x)\ g(x)$ *i.e.*, $c(x)$ is a divisor of $d(x)$.

Thus $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.

Note: If $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$ then any associate of $d(x)$ *i.e.*, $k\ d(x)$ where $0 \neq k \in F$ will also be a greatest common divisor of $f(x)$ and $g(x)$. In particular if $0 \neq b$ is the leading coefficient of the polynomial $d(x)$, then the monic polynomial $b^{-1}d(x)$ will also be a greatest common divisor of $f(x)$ and $g(x)$.

Often while defining greatest common divisor of two polynomials over a field we include one more condition in our definition that the greatest common divisor should be a monic polynomial. The advantage of this extra condition is that now we shall get a unique greatest common divisor as shown below:

Suppose $d_1(x)$ and $d_2(x)$ are two monic polynomials and each is a greatest common divisor of $f(x)$ and $g(x)$. Then $d_1(x) \mid d_2(x)$ and $d_2(x) \mid d_1(x)$. Therefore $d_1(x)$ and $d_2(x)$ are associates and we have $d_1(x) = ud_2(x)$ for some $0 \neq u \in F$. Since $d_1(x)$ and $d_2(x)$ are both monic, therefore $u = 1$.

18 Unique Factorization Domain

Definition: *An integral domain, R, with unity element* 1 *is a unique factorization domain if*

(*a*) *any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible (prime) elements of R;*

(*b*) *the decomposition in part* (*a*) *is unique upto the order and associates of the irreducible elements.*

Thus if R is a unique factorization domain and if $a \neq 0$ is a non-unit in R, then a can be expressed as a product of a finite number of prime elements of R. Also if

$$a = p_1\ p_2\ p_3 \cdots p_n = p_1'\ p_2'\ p_3' \cdots p_m'$$

where the p_i and p_j' are prime elements of R, then $m = n$ and each p_i, $1 \leq i \leq n$ is an associate of some p_j', $1 \leq j \leq m$ and conversely each p_k' is an associate of some p_l.

19 The Unique Factorization Theorem for Polynomials over a Field

We shall now prove that every polynomial over a field can be factored uniquely into irreducible factors. Before stating the main factorization theorem, we shall give two preliminary theorems that are needed for its proof.

Theorem 1: *Let* $f(x)$, $g(x)$ *and* $h(x)$ *be polynomials in* $F[x]$ *for a field* F. *If* $f(x) \mid g(x)\ h(x)$ *and the greatest common divisor of* $f(x)$ *and* $g(x)$ *is* 1, *then* $f(x) \mid h(x)$.

Proof: If the greatest common divisor of $f(x)$ and $g(x)$ is 1, then by theorem of article 17 there exist polynomials $m(x)$ and $n(x) \in F[x]$ such that

$$1 = m(x)\ f(x) + n(x)\ g(x).$$

Multiplying both members of this equation by $h(x)$, we get

$$h(x) = m(x)\ f(x)\ h(x) + n(x)\ g(x)\ h(x) \qquad ...(1)$$

But $f(x) \mid g(x)\ h(x)$, so there exists a polynomial $q(x) \in F[x]$ such that

$$g(x)\ h(x) = q(x)\ f(x).$$

Substituting this value of $g(x)\ h(x)$ in (1), we get

$$\begin{aligned} h(x) &= m(x)\ f(x)\ h(x) + n(x)\ q(x)\ f(x) \\ &= f(x)\ [m(x)\ h(x) + n(x)\ q(x)], \end{aligned}$$

which shows that $f(x)$ is a divisor of $h(x)$.

Hence the theorem.

Theorem 2: *If $f(x)$ is an irreducible polynomial in $F[x]$ for a field F and $f(x) \mid g(x)\ h(x)$ where $g(x), h(x) \in F[x]$ then $f(x)$ divides at least one of $g(x)$ or $h(x)$.*

Proof: Suppose that $f(x)$ does not divide $g(x)$. Since $f(x)$ is prime therefore $f(x)$ does not divide $g(x)$ implies that $f(x)$ and $g(x)$ are relatively prime. Therefore the greatest common divisor of $f(x)$ and $g(x)$ is 1. Hence by theorem 1, we get that $f(x) \mid h(x)$.

Corollary: *If $f(x)$ is an irreducible polynomial in $F[x]$ for a field F, and if $f(x)$ divides the product $g_1(x)\ g_2(x) \ldots g_n(x)$ of polynomials in $F[x]$, then $f(x)$ divides $g_i(x)$ for some i, $1 \le i \le n$.*

This result follows immediately by repeated application of theorem 2.

Theorem 3: The Unique Factorization Theorem for Polynomials over a Field: *Let $f(x)$ be a non-zero polynomial in $F[x]$, where F is a field. Then either $f(x)$ is a unit in $F[x]$ or $f(x) = a(x)\ p_1(x)\ p_2(x) \ldots p_m(x)$, where each $p_i(x)$, $1 \le i \le m$, is an irreducible monic polynomial in $F[x]$ and $a \in F$ is the leading coefficient of $f(x)$. Further the factors $p_1(x), p_2(x), \ldots, p_m(x)$ are unique except for the order in which they appear.*

Proof: We shall prove the theorem in two parts. First we shall prove that $f(x)$ can be factored as required, and then we shall show that the factors are unique.

Let $f(x)$ be a non-zero element of $F[x]$. Then either $f(x)$ is a unit in $F[x]$ *i.e.*, deg $f(x)$ is 0 or deg $f(x) > 0$. If deg $f(x) > 0$, and the leading coefficient of $f(x)$ is a we are to prove that $f(x)$ can be expressed as a product of a and a finite number of irreducible monic polynomials in $F[x]$. The proof will be by induction on the degree of $f(x)$.

Suppose $f(x)$ is of degree one. Let $f(x) = b + ax$ for $a, b \in F$ and $a \neq 0$. We can write $f(x) = a(a^{-1}b + x)$. Therefore the theorem holds in the case where $f(x)$ has degree one since $a^{-1}b + x$ is irreducible and monic.

Now assume, as the induction hypothesis, that every polynomial of degree less than n can be factored as stated in the theorem. Consider an arbitrary polynomial $f(x)$ of degree n having a as its leading coefficient. We can write $f(x) = a\ f_1(x)$, where $f_1(x) = a^{-1} f(x)$ and $f_1(x)$ is monic. If $f(x)$ is irreducible, then $f_1(x)$ is also

irreducible and the theorem holds. If $f(x)$ is reducible, then it can be factored as $f(x) = g(x)\, h(x)$ where neither $g(x)$ nor $h(x)$ is a unit in $F[x]$. Now the degree of $f(x)$ is equal to the sum of the degrees of $g(x)$ and $h(x)$. Also $g(x)$ and $h(x)$ are not units in $F[x]$, so each of them must be of degree one or larger. Hence both $g(x)$ and $h(x)$ have degrees less than n. Therefore by our induction hypothesis we can write

$$g(x) = c\alpha_1(x)\,\alpha_2(x)\ldots\alpha_s(x),\quad h(x) = d\,\beta_1(x)\,\beta_2(x)\ldots\beta_t(x)$$

where each $\alpha_i(x)$ and each $\beta_j(x)$ is monic and irreducible and where c and d are leading coefficients of $g(x)$ and $h(x)$ respectively.

Thus $$f(x) = cd\alpha_1(x)\,\alpha_2(x)\,\alpha_3(x)\ldots\alpha_s(x)\,\beta_1(x)\,\beta_2(x)\ldots\beta_t(x).$$

Since the leading coefficient of $f(x)$ is a, therefore we must have $a = cd$ because each $\alpha(x)$ and each $\beta(x)$ is monic. Therefore

$$f(x) = a\,\alpha_1(x)\,\alpha_2(x)\ldots\alpha_s(x)\,\beta_1(x)\,\beta_2(x)\ldots\beta_t(x).$$

The factorization of $f(x)$ satisfies the requirements of the theorem. Hence the theorem holds for all polynomials of degree n, and by the principle of induction, for all polynomials of arbitrary degree.

In order to prove that the factors are unique, let us suppose that $f(x) = a\,p_1(x)\,p_2(x)\ldots p_m(x) = a\,q_1(x)\,q_2(x)\ldots q_n(x)$ where each $p(x)$ and each $q(x)$ is irreducible and monic. Then we shall prove that $n = m$ and each $p(x)$ is equal to some $q(x)$ and each $q(x)$ is equal to some $p(x)$. From these two decompositions of $f(x)$, we have

$$p_1(x)\,p_2(x)\ldots p_m(x) = q_1(x)\,q_2(x)\ldots q_n(x).$$

Now $$p_1(x) \mid p_1(x)\,p_2(x)\ldots p_m(x).$$

Therefore $$p_1(x) \mid q_1(x)\,q_2(x)\ldots q_n(x).$$

By corollary to theorem 2 of this article $p_1(x)$ must divide at least one of $q_1(x), q_2(x), \ldots, q_n(x)$. Since $F[x]$ is a commutative ring, therefore without loss of generality we may suppose that $p_1(x)$ divides $q_1(x)$. But $p_1(x)$ and $q_1(x)$ are both irreducible polynomials in $F[x]$ and $p_1(x) \mid q_1(x)$. Therefore $p_1(x)$ and $q_1(x)$ must be associates and we have $q_1(x) = u\,p_1(x)$ where u is a unit in $F[x]$ *i.e.*, u is a non-zero element of F. Since $q_1(x)$ and $p_1(x)$ are monic therefore u must be equal to 1 and we have $p_1(x) = q_1(x)$. Thus we have

$$p_1(x)\,p_2(x)\ldots p_m(x) = p_1(x)\,q_2(x)\ldots q_n(x).$$

Cancelling $0 \neq p_1(x)$ from both sides, we get

$$p_2(x)\,p_3(x)\ldots p_m(x) = q_2(x)\,q_3(x)\ldots q_n(x) \qquad \ldots(1)$$

Now we can repeat the above argument on the relation (1) with $p_2(x)$. If $n > m$, then after m steps the left hand side becomes 1 while the right hand side reduces to a product of a certain number of $q(x)$ (the excess of n over m). But the $q(x)$ are irreducible polynomials so they are not units of $F[x]$ *i.e.*, they are not polynomials of zero degree.

So their product will be a polynomial of degree ≥ 1. So it cannot be equal to 1. Therefore n cannot be greater than m. Then $n \leq m$. Similarly interchanging the roles

of $p(x)$ and $q(x)$, we get $m \leq n$. Hence $m = n$.

Also in the above process we have shown that every $p(x)$ is equal to some $q(x)$ and conversely every $q(x)$ is equal to some $p(x)$. Hence the theorem has been completely established.

Thus we can say that *the ring of polynomials over a field is a unique factorization domain.*

20 Value of a Polynomial at $x = c$

Definition: *Let* $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ *be a polynomial in* $F[x]$ *for an arbitrary field* F *and let* c *be an element of* F. *Then*

$$f(c) = a_0 + a_1 c + a_2 c^2 + \ldots + a_n c^n,$$

where the indicated addition and multiplication are the operations in F, *is called the value of* $f(x)$ *at* $x = c$.

Obviously $f(c)$ is an element of F.

Zeros of a polynomial: Definition: *If* $f(x)$ *is a polynomial in* $F[x]$ *for an arbitrary field* F, *and* $f(c) = 0$ *for an element* $c \in F$, *then* c *is called a zero of* $f(x)$.

Polynomial equations and their roots:

Definition: *Let* $f(x)$ *be a polynomial of degree* n *over a field* F. *We say that* $f(x) = 0$ *is an equation over the field* F *and* n *is the degree of the equation.*

If c *is a zero of the polynomial* $f(x)$, *then* c *is a root of the equation* $f(x) = 0$. A root of an equation is also called a **solution** of the equation.

Remainder Theorem: *If* $f(x) \in F[x]$ *and* $a \in F$, *for any field* F, *then* $f(a)$ *is the remainder when* $f(x)$ *is divided by* $(x - a)$.

Proof: By division algorithm there exist polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)(x - a) + r(x)$, where either $r(x) = 0$ or deg $r(x)$ is less than the degree of $x - a$. But the degree of $(x - a)$ is 1. Therefore $r(x)$ has degree 0 or no degree. Hence $r(x)$ is a constant polynomial *i.e.*, $r(x)$ is simply an element, say, r in F. Thus $f(x) = q(x)(x - a) + r$. Putting $x = a$ in this relation, we get

$$f(a) = q(a)(a - a) + r \Rightarrow f(a) = r.$$

Corollary: Factor Theorem: *If* $f(x) \in F[x]$ *and* $a \in F$, *for a field* F, *then* $x - a$ *divides* $f(x)$ *if and only if* $f(a) = 0$.

Proof: By remainder theorem, $f(a)$ is the remainder when $f(x)$ is divided by $(x - a)$. Therefore if $f(a) = 0$, then $(x - a)$ divides $f(x)$.

Conversely, if $f(x)$ is divisible by $(x - a)$ we get

$$f(x) = (x - a)\, q(x).$$

Putting $x = a$, we get

$$f(a) = (a - a)\, q(a) = 0 \; q(a) = 0.$$

Illustrative Examples

Example 7: *Show that the polynomial* $x^2 + x + 4$ *is irreducible over* F, *the field of integers modulo* 11.

Solution: The field F is $(\{0, 1, ..., 10\}, +_{11}, \times_{11})$.

Let $f(x) = x^2 + x + 4$.

If $a \in F$, then by a^n we shall mean $a \times_{11} a \times_{11} a \times_{11} a...$ upto n times.

Now $f(0) = 0^2 +_{11} 0 +_{11} 4 = 4, f(1) = 1^2 +_{11} 1 +_{11} 4 = 6,$
$f(2) = 2^2 +_{11} 2 +_{11} 4 = 10, f(3) = 3^2 +_{11} 3 +_{11} 4 = 5, f(4) = 2,$
$f(5) = 1, f(6) = 6^2 +_{11} 6 +_{11} 4 = 2, f(7) = 5, \ f(8) = 10, \ f(9) = 6,$
$f(10) = 4.$

Since $f(a) \neq 0 \ \forall \ a \in F$, therefore by factor theorem $x - a$ does not divide $f(x) \ \forall \ a \in F$. Therefore $f(x)$ has no proper divisors in $F[x]$. Hence $f(x)$ is irreducible over F.

Comprehensive Exercise 1

1. Resolve $x^4 + 4$ into factors over the field $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$.
2. Resolve $x^2 + 1$ into factors over the field Z_5.
3. Find the solution of the equation $3x = 2$ in the field $(Z_7, +_7, \times_7)$.
4. Show that $f(x) = x^2 + 8x - 2$ is irreducible over the field of rational numbers **Q.** Is it irreducible over reals ? Give reasons for your answer.
5. Let $f(x) = 2x^4 + 3x^3 + 2$ and $g(x) = 3x^5 + 4x^3 + 2x^2 + 3$ be two polynomials over the field $Z_5 = (\{0, 1, 2, 3, 4\}, +_5, \times_5)$.

 Determine (i) $\frac{d}{dx} f(x)$, (ii) $f(x) \cdot g(x)$.
6. If $f(x) = 3x^7 + 2x + 3$, $g(x) = 5x^3 + 2x + 6$ be two polynomials over the field $Z_7 = (\{0, 1, 2, 3, 4, 5, 6\}, +_7, \times_7)$, determine

 (i) $\frac{d}{dx} f(x)$, (ii) $f(x) \cdot g(x)$, and (iii) $f(x) + g(x)$.
7. Let $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ be in $Z_7[x]$. Find

 (i) Sum and product of $f(x)$ and $g(x)$ in $Z_7[x]$.

 (ii) Two polynomials $q(x)$ and $r(x)$ in $Z_7[x]$ such that $f(x) = q(x) \ g(x) + r(x)$ with degree $r(x) < 2$.

Answers 1

1. $x^4 + 4 = (x + 1)(x + 2)(x + 3)(x + 4)$.

2. $x^2 + 1 = (x + 2)(x + 3)$.

3. $x = 3$ because $3 \times_7 3 \times_7 3 = 2$.

4. not irreducible over reals.

5. (i) $3x^3 + 4x^2$.

(ii) $1 + 4x^2 + 2x^3 + x^4 + 2x^5 + x^6 + 3x^7 + 4x^8 + x^9$.

6. (i) 2

(ii) $4 + 4x + 4x^2 + x^3 + 3x^4 + 4x^7 + 6x^8 + x^{10}$.

(iii) $3x^7 + 5x^3 + 4x + 2$.

7. (i) $f(x) + g(x) = x^6 + 3x^5 + 5x^2 + 6x + 6$.

$f(x)\, g(x) = x^8 + 5x^7 + 3x^6 + 5x^5 + 4x^4 + 5x^3 + 5x^2 + 6x + 1$

Note that in Z_7, we have $-3 = 4$, $-1 = 6$ etc.

(ii) $q(x) = x^4 + x^3 + x^2 + x + 5$, $r(x) = 4x + 3$.

21 Maximal Ideal

An ideal $S \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $S \subseteq U \subseteq R$, then either $R = U$ or $S = U$.

In other words an ideal S of a ring R is said to be *maximal ideal* if there exists no ideal properly contained in R which itself properly contains S *i.e.*, if it is impossible to find an ideal which lies between S and the full ring R. For example, in the ring of integers **I**, the ideal (6) is not maximal since it is properly contained in the ideal (3), which in turn is properly contained in **I**. On the other hand, (5) is a maximal ideal since the only ideal properly containing (5) is **I** itself.

Theorem: *An ideal S of the ring of integers **I** is maximal if and only if S is generated by some prime integer.*

Proof: We know that every ideal of the ring of integers **I** is a principal ideal. Suppose S is an ideal of **I** generated by p so that $S = (p)$. Since p and $-p$ generate the same ideal, therefore we can take p as positive.

Now we are to prove that

(i) S is maximal if p is prime.

(ii) p is prime if S is maximal.

First we shall prove (i). Let p be a prime integer such that $(p) = S$. Let T be an ideal of **I** such that $S \subseteq T \subseteq \mathbf{I}$. Since T is also a principal ideal of **I**, let $T = (q)$ where q is some positive integer.

Now $\quad S \subseteq T \quad \Rightarrow \quad (p) \subseteq T \quad \Rightarrow \quad p \in T$

$\Rightarrow \quad p \in \{xq : x \in \mathbf{I}\} \quad \Rightarrow \quad p = rq$ for some positive integer r.

Since p is prime, therefore $q = 1$ or $q = p$.

If $q = 1$, we have $T = (q) = (1) = \mathbf{I}$

and if $q = p$, we have $T = (q) = (p) = S$.

Thus either $T = \mathbf{I}$ or $T = S$.

Hence (p) is a maximal ideal of $\mathbf{I}$.

Now we shall prove (ii). Let $(p) = S$ be a maximal ideal. We are to show that p is prime. Let us suppose that p is a composite integer.

Let $p = mn, \ m \neq 1, \ n \neq 1$.

It is obvious that $(p) \subseteq (m) \subseteq \mathbf{I}$.

But since (p) is a maximal ideal, therefore we have

either $(m) = (p)$ or $(m) = \mathbf{I}$.

If $(m) = \mathbf{I}$, then $m = 1$, which is a contradiction.

If $(m) = (p)$, then m must be equal to lp for some integer l since each element of (p) is a multiple of p.

Therefore $p = mn = lpn = pln$. But $p \neq 0$, therefore $ln = 1$. This gives $n = 1$ which is again a contradiction.

Hence p must be a prime integer.

22 More Results on Ideals

Theorem 1: *Let S_1, S_2 be ideals of a ring R and let*

$$S_1 + S_2 = \{s_1 + s_2 : s_1 \in S_1, s_2 \in S_2\}.$$

Then $S_1 + S_2$ is an ideal of R generated by $S_1 \cup S_2$.

Proof: Let $a_1 + a_2 \in S_1 + S_2, b_1 + b_2 \in S_1 + S_2$. Then

$$a_1, b_1 \in S_1 \text{ and } a_2, b_2 \in S_2.$$

We have $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2)$.

Since S_1 is an ideal, therefore $a_1, b_1 \in S_1 \Rightarrow a_1 - b_1 \in S_1$.

Similarly $a_2 - b_2 \in S_2$.

$\therefore \quad (a_1 - b_1) + (a_2 - b_2) \in S_1 + S_2$.

$\therefore \quad (a_1 + a_2) - (b_1 + b_2) \in S_1 + S_2$.

$\therefore \ S_1 + S_2$ is a subgroup of the additive group of R.

Let r be any element of R. Then

$$r(a_1 + a_2) = ra_1 + ra_2 \in S_1 + S_2;$$

since $r \in R, a_1 \in S_1 \Rightarrow ra_1 \in S_1$ and similarly $ra_2 \in S_2$.

Similarly $(a_1 + a_2)r = a_1 r + a_2 r \in S_1 + S_2$,

since $a_1 r \in S_1, a_2 r \in S_2$.

Hence $S_1 + S_2$ is an ideal of R.

Since $0 \in S_1$ and also $0 \in S_2$, therefore obviously

$$S_1 \subseteq S_1 + S_2 \text{ and } S_2 \subseteq S_1 + S_2 .$$

$\therefore$ $\quad S_1 \cup S_2 \subseteq S_1 + S_2 .$

Thus $S_1 + S_2$ is an ideal of R containing $S_1 \cup S_2$.

Also if S is any ideal of R containing $S_1 \cup S_2$, then S must contain $S_1 + S_2$. Thus $S_1 + S_2$ is the smallest ideal of R containing $S_1 \cup S_2$ *i.e.*,

$$S_1 + S_2 = (S_1 \cup S_2).$$

Theorem 2: *If an ideal U of a ring R contains a unit of R then $U = R$.*

(Gorakhpur 2013)

Proof: Let R be a ring with unity element 1. Let u be a unit of R. Then u is an inversible element of R *i.e.*, u^{-1} exists. Let $u \in U$.

Since U is an ideal, therefore

$$u \in U,\ u^{-1} \in R \ \Rightarrow\ uu^{-1} \in U \ \Rightarrow\ 1 \in U.$$

Now let x be any element of R. Then

$$x \in R, 1 \in U \ \Rightarrow\ x\,1 \in U \ \Rightarrow\ x \in U.$$

$\therefore$ $\quad R \subseteq U.$

Also $U \subseteq R$ as U is an ideal of R. Hence $R = U$.

Theorem 3: *Let R be a commutative ring with unity and a, b be two non-zero elements of R. Then $(a) = (b)$ iff $a \mid b$ and $b \mid a$.*

Proof: Here (a) = the principal ideal of R generated by a

$$= \{ ax \ : \ x \in R \}.$$

Similarly $\quad (b)$ = the principal ideal of R generated by b.

Let $\quad (a) = (b)$.

Then $\quad (a) \subseteq (b) \quad \Rightarrow \quad a \in (b)$

$\Rightarrow$ $\quad a = rb$ for some $r \in R$

$\Rightarrow$ $\quad b \mid a$ *i.e.*, b is a divisor of a.

Similarly $\quad (a) = (b)$

$\Rightarrow$ $\quad (b) \subseteq (a) \quad \Rightarrow \quad b \in (a)$

$\Rightarrow$ $\quad b = sa$ for some $s \in R \Rightarrow a \mid b$.

Thus $\quad (a) = (b) \quad \Rightarrow \quad a \mid b$ and $b \mid a$.

Conversely let $a \mid b$ and $b \mid a$.

Now $\ a \mid b \Rightarrow b = pa$ for some $p \in R$. Let y be any element of (b).

Then $\quad y = ub$ for some $u \in R$

$$= u\,(\,pa) = (up)\,a \in (a) \text{ since } up \in R.$$

Thus $\quad y \in (b) \quad \Rightarrow \quad y \in (a)$.

$\therefore$ $\quad (b) \subseteq (a)$.

Thus $\quad a \mid b \quad \Rightarrow \quad (b) \subseteq (a)$.

Similarly $b \mid a \Rightarrow (a) \subseteq (b)$.

Consequently $a \mid b, b \mid a \Rightarrow (a) = (b)$.

Corollary: *Let R be an integral domain with unity and a, b be two non-zero elements of R. Then* $(a) = (b)$ *iff a and b are associates.*

Theorem 4: *An ideal S of a commutative ring R with unity is maximal if and only if the residue class ring R / S is a field.*

Proof: Since R is a commutative ring with unity, therefore R/S is also a commutative ring with unity. The zero element of the ring R/S is S and the unity element is the coset $S + 1$ where 1 is the unity element of R.

Let the ideal S be maximal. Then to prove that R/S is a field.

Let $S + b$ be any non-zero element of R/S. Then $S + b \neq S$ *i.e.*, $b \notin S$. To prove that $S + b$ is inversible.

If (b) is the principal ideal of R generated by b, then $S + (b)$ is also an ideal of R. Since $b \notin S$, therefore the ideal S is properly contained in $S + (b)$. But S is a maximal ideal of R. Hence we must have $S + (b) = R$.

Since $1 \in R$, therefore we must obtain 1 on adding an element of S to an element of (b). Therefore there exists an element $a \in S$ and $\alpha \in R$ such that

$$a + \alpha b = 1 \qquad [\text{Note that } (b) = \{\alpha b : \alpha \in R\}]$$

$$\therefore \quad 1 - \alpha b = a \in S.$$

Consequently $S + 1 = S + \alpha b = (S + \alpha)(S + b)$.

$$\therefore \quad S + \alpha = (S + b)^{-1}.$$

Thus $S + b$ is inversible.

$\therefore$ R/S is a field.

Conversely, let S be an ideal of R such that R/S is a field. We shall prove that S is a maximal ideal of R.

Let S' be an ideal of R properly containing S *i.e.*, $S \subseteq S'$ and $S \neq S'$. Then S will be maximal if $S' = R$. The elements of R contained in S already belong to S' since $S \subseteq S'$. Therefore R will be a subset of S' if every element α of R not contained in S also belongs to S'. If $\alpha \in R$ is such that $\alpha \notin S$, then $S + \alpha \neq S$ *i.e.*, $S + \alpha$ is a non-zero element of R/S. Also S' properly contains S. Therefore there exists an element β of S' not contained in S so that $S + \beta$ is also a non-zero element of R/S. Now the non-zero elements of R/S form a group with respect to multiplication because R/S is a field. Therefore there exists a non-zero element $S + y$ of R/S such that

$$(S + y)(S + \beta) = S + \alpha. \quad [\text{We may take } S + y = (S + \alpha)(S + \beta)^{-1}]$$

Now $(S + y)(S + \beta) = S + \alpha$

$$\Rightarrow \quad S + y\beta = S + \alpha \Rightarrow y\beta - \alpha \in S \Rightarrow y\beta - \alpha \in S'. \qquad [\because S \subseteq S']$$

Now S' is an ideal. Therefore

$y \in R, \beta \in S' \Rightarrow y\beta \in S'$.

Again $y\beta \in S', y\beta - \alpha \in S' \Rightarrow y\beta - (y\beta - \alpha) \in S'$ *i.e.*, $\alpha \in S'$.

Thus $R \subseteq S'$.

Also $S' \subseteq R$ as S' is an ideal of R.

$\therefore$ $S' = R$.

Hence the theorem.

23 Prime Ideals

Prime Ideal: Definition: *Let R be a ring and S an ideal in R. Then S is said to be a prime ideal of R if* $ab \in S$, $a, b \in R$ *implies that either a or b is in S.*

For example, in the ring of integers **I**, the principal ideal (7) is prime. Obviously if ab is in (7), then a or b must be a multiple of 7. On the other hand, (6) is not a prime ideal in **I** since, in particular, $12 = 3 \times 4$ is in (6), yet neither 3 nor 4 is an element of (6).

Theorem 1: *Let R be a commutative ring and S an ideal of R. Then the ring of residue classes R / S is an integral domain if and only if S is a prime ideal.* **(Gorakhpur 2011)**

Proof: Let R be a commutative ring and S an ideal of R. Then

$R / S = \{S + a : a \in R\}$.

Let $S + a, S + b$ be any two elements of R / S. Then $a, b \in R$.

We have $(S + a)(S + b) = S + ab$

$= S + ba$ [$\because$ R is a commutative ring]

$= (S + b)(S + a)$.

$\therefore$ R / S is a commutative ring.

Now let S be a prime ideal of R. Then we are to prove that R / S is an integral domain. For this we are to show that R / S is without zero divisors. The zero element of the ring R / S is the residue class S itself. Let $S + a, S + b$ be any two elements of R / S.

Then $(S + a)(S + b) = S$ (the zero element of R / S)

$\Rightarrow$ $S + ab = S \Rightarrow ab \in S$

$\Rightarrow$ either a or b is in S, since S is a prime ideal

$\Rightarrow$ either $S + a = S$ or $S + b = S$ [Note that $a \in S \Leftrightarrow S + a = S$]

$\Rightarrow$ either $S + a$ or $S + b$ is the zero element of R / S.

$\therefore$ R / S is without zero divisors.

Since R / S is a commutative ring without zero divisors, therefore R / S is an integral domain.

Conversely, let R / S be an integral domain. Then we are to prove that S is a prime ideal of R. Let a, b be any two elements in R such that $ab \in S$. We have

$ab \in S \Rightarrow S + ab = S \Rightarrow (S + a)(S + b) = S$.

Since R / S is an integral domain, therefore it is without zero divisors. Therefore

$(S + a)(S + b) = S$ (the zero element of R / S)

$\Rightarrow$ either $S + a$ or $S + b$ is zero

$\Rightarrow$ either $S + a = S$ or $S + b = S$

$\Rightarrow$ either $a \in S$ or $b \in S$

$\Rightarrow$ S is a prime ideal.

This completes the proof of the theorem.

Note: If R is a ring with unity, then R / S is also a ring wity unity. The residue class $S + 1$ is the unity element of R / S. Therefore if we define an integral domain as a commutative ring with unity and without zero divisors, even then the above theorem will be true. But in that case R must be a commutative ring with unity.

Theorem 2: *Let R be a commutative ring with unity. Then every maximal ideal of R is a prime ideal.*

Proof: R is a commutative ring with unit element. Let S be a maximal ideal of R. Then R / S is a field.

Now every field is an integral domain. Therefore R / S is also an integral domain. Hence by theorem 1, S is a prime ideal of R. This completes the proof of the theorem.

But it should be noted that the converse of the above theorem is not true *i.e.*, every prime ideal is not necessarily a maximal ideal.

Illustrative Examples

Example 8: *Let* **R** *be the field of real numbers and S the set of all those polynomials* $f(x) \in \mathbf{R}[x]$ *such that* $f(0) = 0 = f(1)$. *Prove that S is an ideal of* $\mathbf{R}[x]$. *Is the residue class ring* $\mathbf{R}[x] / S$ *an integral domain? Give reasons for your answer.*

Solution: Let $f(x)$, $g(x)$ be any elements of S. Then

$f(0) = 0 = f(1)$ and $g(0) = 0 = g(1)$.

Let $h(x) = f(x) - g(x)$.

Then $h(0) = f(0) - g(0) = 0 - 0 = 0$ and $h(1) = f(1) - g(1) = 0 - 0 = 0$.

Thus $h(0) = 0 = h(1)$.

Therefore $h(x) \in S$.

Thus $f(x), g(x) \in S \Rightarrow h(x) = f(x) - g(x) \in S$.

Further let $f(x)$ be any element of S and $r(x)$ be any element of $\mathbf{R}[x]$.

Then $f(0) = 0 = f(1)$, by definition of S.

Let $t(x) = r(x) f(x) = f(x) r(x)$. [$\because$ $\mathbf{R}[x]$ is a commutative ring]

Then $t(0) = r(0) f(0) = r(0) . 0 = 0$

and $t(1) = r(1) f(1) = r(1) . 0 = 0$.

$\therefore$ $t(x) \in S$.

Thus $r(x) \in \mathbf{R}[x], f(x) \in S \Rightarrow r(x) f(x) \in S$.

Hence S is an ideal of $\mathbf{R}[x]$.

Now we claim that S is not a prime ideal of $\mathbf{R}[x]$. Let $f(x) = x(x-1)$. Then $f(0) = 0(0-1) = 0$, and $f(1) = 1(1-1) = 0$.

Thus $f(x) = x(x-1)$ is an element of S.

Now let $p(x) = x$, $q(x) = x - 1$.

We have $p(1) = 1 \neq 0$. Therefore $p(x) \notin S$. Also

$$q(0) = 0 - 1 = -1 \neq 0.$$

Therefore $q(x) \notin S$. Thus $x(x-1) \in S$ while neither $x \in S$ nor $x - 1 \in S$. Hence S is not a prime ideal of $\mathbf{R}[x]$.

Since S is not a prime ideal of $\mathbf{R}[x]$, therefore the residue class ring $\mathbf{R}[x]/S$ is not an integral domain.

Example 9: *Let R be the ring of all real valued continuous functions defined on the closed interval $[0,1]$. Let $M = \{f(x) \in R : f\left(\frac{1}{3}\right) = 0\}$.*

Show that M is a maximal ideal of R.

Solution: First of all we observe that M is non-empty because the real valued function $e(x)$ on $[0, 1]$ defined by

$$e(x) = 0 \quad \forall \quad x \in [0, 1]$$

belongs to M.

Now let $f(x)$, $g(x)$ be any two elements of M. Then

$$f\left(\frac{1}{3}\right) = 0,\ g\left(\frac{1}{3}\right) = 0, \text{ by definition of } M.$$

Let $h(x) = f(x) - g(x)$.

Then $$h\left(\frac{1}{3}\right) = f\left(\frac{1}{3}\right) - g\left(\frac{1}{3}\right) = 0 - 0 = 0.$$

Therefore $h(x) \in M$.

Thus $f(x), g(x) \in M \Rightarrow h(x) = f(x) - g(x) \in M$.

Further let $f(x)$ be any element of M and $r(x)$ be any element of R. Then

$$f\left(\frac{1}{3}\right) = 0, \text{ by definition of } M.$$

Let $t(x) = r(x) f(x) = f(x) r(x)$. [$\because$ R is a commutative ring.]

Then $t\left(\frac{1}{3}\right) = r\left(\frac{1}{3}\right) f\left(\frac{1}{3}\right) = r\left(\frac{1}{3}\right).0 = 0$. Therefore $t(x) \in M$.

Thus $r(x) \in R, f(x) \in M \Rightarrow r(x) f(x) \in M$.

Hence M is an ideal of R.

Clearly $M \neq R$ because $i(x) \in R$ given by $i(x) = 1 \ \forall \ x \in [0, 1]$ does not belong to M.

The ring R is with unity and the element $i(x)$ is its unity element.

Let N be an ideal of R properly containing M *i.e.*, $M \subseteq N$ and $M \neq N$. Then M will be a maximal ideal of R if $N = R$, which will be so if the unity $i(x)$ of R belongs to N. Since M is a proper subset of N, therefore there exists $\lambda(x) \in N$ such that $\lambda(x) \notin M$. This means $\lambda\left(\frac{1}{3}\right) \neq 0$. Put $\lambda\left(\frac{1}{3}\right) = c$ where $c \neq 0$.

Let us define $\beta(x) \in R$ by $\beta(x) = c \ \forall\ x \in [0, 1]$. Now consider $\mu(x) \in R$ given by

$$\mu(x) = \lambda(x) - \beta(x).$$

We have $$\mu\left(\frac{1}{3}\right) = \lambda\left(\frac{1}{3}\right) - \beta\left(\frac{1}{3}\right) = c - c = 0.$$

Therefore $\mu(x) \in M$ and so $\mu(x)$ also belongs to N because N is a super-set of M. Now N is an ideal of R and $\lambda(x), \mu(x)$ are in N. Therefore $\lambda(x) - \mu(x) = \beta(x)$ is also an element of N.

Now define $\gamma(x) \in R$ by $\gamma(x) = 1/c \ \ \forall \ \ x \in [0, 1]$. Since N is an ideal of R, therefore $\gamma(x) \in R$ and $\beta(x) \in N \ \Rightarrow\ \gamma(x)\,\beta(x) \in N$. We shall show that $\gamma(x)\,\beta(x) = i(x)$.

For every $x \in [0, 1]$, we have $\gamma(x)\,\beta(x) = (1/c)\,c = 1$.

Therefore $\gamma(x)\,\beta(x) = i(x)$, by definition of $i(x)$.

Thus the unity element $i(x)$ of R belongs to N and consequently $N = R$.

Hence M is a maximal ideal of R.

Example 10: *If R is a finite commutative ring (i.e., has only a finite number of elements) with unit element prove that every prime ideal of R is a maximal ideal of R.*

Solution: Let R be a finite commutative ring with unit element. Let S be a prime ideal of R. Then to prove that S is a maximal ideal of R.

Since S is a prime ideal of R, therefore the residue class ring R/S is an integral domain. Now

$$R/S = \{S + a \ : \ a \in R\}.$$

Since R is a finite ring, therefore R/S is a finite integral domain. But every finite integral domain is a field. Therefore R/S is a field. Since R is a commutative ring with unity and R/S is a field, therefore S is a maximal ideal of R.

Example 11: *Give an example of a ring in which some prime ideal is not a maximal ideal.*

Solution: Let $\mathbf{I}[x]$ be the ring of polynomials over the ring of integers $\mathbf{I}$. Let S be the principal ideal of $\mathbf{I}[x]$ generated by x *i.e.*, let $S = (x)$. We shall show that (x) is prime but not maximal.

We have $$S = (x) = \{x\, f(x) \ : \ f(x) \in \mathbf{I}[x]\}.$$

First we shall prove that S is prime.

Let $a(x), b(x) \in \mathbf{I}[x]$ be such that $a(x)\,b(x) \in S$. Then there exists a polynomial $c(x) \in \mathbf{I}[x]$ such that

$$x\,c(x) = a(x)\,b(x). \qquad \ldots(1)$$

Let $$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots,\ b(x) = b_0 + b_1 x + b_2 x^2 + \ldots,$$

$$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots.$$

Then (1) becomes

$$x(c_0 + c_1x + \ldots) = (a_0 + a_1x + \ldots)(b_0 + b_1x + \ldots).$$

Equating the constant term on both sides, we get

$$a_0\, b_0 = 0 \Rightarrow a_0 = 0 \text{ or } b_0 = 0. \quad [\because \mathbf{I} \text{ is without zero divisors}]$$

Now $a_0 = 0 \Rightarrow a(x) = a_1x + a_2x^2 + \ldots$

$\Rightarrow$ $a(x) = x(a_1 + a_2x + \ldots) \Rightarrow a(x) \in (x)$.

Similarly $b_0 = 0 \Rightarrow b(x) = b_1x + b_2x^2 + \ldots$

$\Rightarrow$ $b(x) = x(b_1 + b_2x + \ldots) \Rightarrow b(x) \in (x)$.

Thus $a(x)\, b(x) \in (x) \Rightarrow$ either $a(x) \in (x)$ or $b(x) \in (x)$.

Hence (x) is a prime ideal.

Now we shall show that (x) is not a maximal ideal of $\mathbf{I}[x]$. For this we must show an ideal N of $\mathbf{I}[x]$ such that (x) is properly contained in N, while N itself is properly contained in $\mathbf{I}[x]$. The ideal $N = (x, 2)$ serves this purpose.

Obviously $(x) \subseteq (x, 2)$. In order to show that (x) is properly contained in $(x, 2)$ we must show an element of $(x, 2)$ which is not in (x). Clearly $2 \in (x, 2)$. We shall show that $2 \notin (x)$. Let $2 \in (x)$. Then we can write,

$$2 = x f(x) \text{ for some } f(x) \in \mathbf{I}[x].$$

Let $f(x) = a_0 + a_1x + \ldots$

Then $2 = x f(x) \Rightarrow 2 = x(a_0 + a_1x + \ldots)$

$\Rightarrow$ $2 = a_0x + a_1x^2 + \ldots \quad \Rightarrow \quad 2 = 0 + a_0x + a_1x^2 + \ldots$

$\Rightarrow$ $2 = 0$ [by equality of two polynomials]

But $2 \neq 0$ in the ring of integers. Hence $2 \notin (x)$. Thus (x) is properly contained in $(x, 2)$.

Now obviously $(x, 2) \subseteq \mathbf{I}[x]$. In order to show that $(x, 2)$ is properly contained in $\mathbf{I}[x]$ we must show an element of $\mathbf{I}[x]$ which is not in $(x, 2)$. Clearly $1 \in \mathbf{I}[x]$. We shall show that $1 \notin (x, 2)$. Let $1 \in (x, 2)$. Then we have a relation of the form

$$1 = x f(x) + 2 g(x), \text{ where } f(x), g(x) \in \mathbf{I}[x].$$

Let $f(x) = a_0 + a_1x + \ldots$, $g(x) = b_0 + b_1x + \ldots$

Then $1 = x(a_0 + a_1x + \ldots) + 2(b_0 + b_1x + \ldots)$

$\Rightarrow$ $1 = 2\, b_0$ [Equating constant term on both sides]

But there is no integer b_0 such that $1 = 2\, b_0$.

Hence $1 \notin (x, 2)$. Thus $(x, 2)$ is properly contained in $\mathbf{I}[x]$.

Therefore (x) is not a maximal ideal of $\mathbf{I}[x]$.

24 Euclidean Rings or Euclidean Domains

Definition: *Let R be an integral domain i.e., let R be a commutative ring without zero divisors. Then R is said to be a Euclidean ring if to every non-zero element $a \in R$ we can assign a non-negative integer $d(a)$ such that*:

(*i*) *For all* $a, b \in R$, *both non-zero,* $d(ab) \geq d(a)$.

(*ii*) *For any* $a, b \in R$ *and* $b \neq 0$, *there exist* $q, r \in R$ *such that* $a = qb + r$ *where either* $r = 0$ *or* $d(r) < d(b)$. **(Lucknow 2007)**

The second part of the above definition is known as **division algorithm**. Also we do not assign a value to $d(0)$. Thus $d(a)$ will remain undefined when $a = 0$. Also $d(a)$ will be called d-value of a and $d(a)$ must be some non-negative integer for every non-zero element $a \in R$.

Illustrative Examples

Example 12: *Show that the ring of integers is a Euclidean ring.*

Solution: Let $(\mathbf{I}, +, .)$ be the ring of integers where

$$\mathbf{I} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Let the d function on the non-zero elements of $\mathbf{I}$ be defined as

$$d(a) = |a| \quad \forall \quad 0 \neq a \in \mathbf{I}.$$

Now if $0 \neq a \in \mathbf{I}$, then $|a|$ is a non-negative integer. Thus we have assigned a non-negative integer to every non-negative element $a \in \mathbf{I}$.

$$[d(-5) = |-5| = 5, d(-1) = |-1| = 1, d(4) = |4| = 4 \text{ etc.}]$$

Further if $a, b \in \mathbf{I}$ and are both non-zero, then

$$|ab| = |a||b| \quad \Rightarrow \quad |ab| \geq |a| \qquad [\because |b| \geq 1 \text{ if } 0 \neq b \in \mathbf{I}]$$

$$\Rightarrow \quad d(ab) \geq d(a).$$

Finally we know that if $a \in \mathbf{I}$ and $0 \neq b \in \mathbf{I}$, then there exist two integers q and r such that

$$a = qb + r \text{ where } 0 \leq r < |b|$$

i.e., where either $r = 0$ or $1 \leq r < |b|$

i.e., where either $r = 0$ or $d(r) < d(b)$.

It should be noted that $d(b) = |b|$ and if r is a positive integer then

$$r = |r| = d(r).$$

Therefore the ring of integers is a Euclidean ring.

Example 13: *Show that the ring of polynomials over a field is a Euclidean ring.* **(Gorakhpur 2010)**

Solution: Let $F[x]$ be the ring of polynomials over a field F. Let the d function on the non-zero polynomials in $F[x]$ be defined as

$$d[f(x)] = \deg f(x), \quad \forall \quad 0 \neq f(x) \in F[x].$$

Now if $0 \neq f(x) \in F[x]$, then $\deg f(x)$ is a non-negative integer.

Thus we have assigned a non-negative integer to every non-zero element $f(x)$ in $F[x]$.

Further if $f(x), g(x) \in F[x]$ and are both non-zero polynomials, then

$$\deg [f(x)\, g(x)] = \deg f(x) + \deg g(x)$$

$\Rightarrow$ $\deg [f(x)\, g(x)] \geq \deg f(x)$ $[\because \deg g(x) \geq 0]$

$\Rightarrow$ $d[f(x)\, g(x)] \geq d[f(x)]$.

Finally we know that if $f(x) \in F[x]$ and $0 \neq g(x) \in F[x]$, then there exist two polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x)\, g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

i.e., where either $r(x) = 0$ or $d[r(x)] < d[g(x)]$.

Hence the ring of polynomials over a field is a Euclidean ring .

Example 14: *Show that every field is a Euclidean ring.* **(Gorakhpur 2010, 12)**

Solution: Let F be any field. Let the d function on the non-zero elements of F be defined as

$$d(a) = 0 \quad \forall \quad 0 \neq a \in F.$$

Thus we have assigned the integer zero to every non-zero element in F.

If a and b are non-zero elements in F then ab is also a non-zero element in F. We have therefore

$$d(ab) = 0 = d(a).$$

Thus we have $d(ab) \geq d(a)$.

Finally if $a \in F$ and $0 \neq b \in F$, then we can write

$$a = (ab^{-1})\, b + 0$$

i.e., $a = qb + r$, where $q = ab^{-1}$ and $r = 0$.

Hence every field is a Euclidean ring.

Example 15: *Show that the ring of Gaussian integers is a Euclidean ring.*

Solution: Let $(G, +, .)$ be the ring of Gaussian integers where

$$G = \{x + iy \ : \ x, y \in \mathbf{I}\}.$$

Let the d function on the non-zero elements of G be defined as

$$d(x + iy) = x^2 + y^2 \quad \forall \quad 0 + i0 \neq x + iy \in G.$$

Now if $x + iy$ is a non-zero element of G, then $(x^2 + y^2)$ is a non-negative integer.

Thus we have assigned a non-negative integer to every non-zero element of G.

If $x + iy$ and $m + in$ are two non-zero elements of G, then

$$d[(x + iy)(m + in)] = d[(xm - ny) + i(my + xn)]$$

$$= (xm - ny)^2 + (my + xn)^2 = x^2 m^2 + n^2 y^2 + m^2 y^2 + x^2 n^2$$

$$= (x^2 + y^2)(m^2 + n^2)$$

$$\geq x^2 + y^2. \qquad [\because m^2 + n^2 \geq 1]$$

Thus $d[(x + iy)(m + in)] \geq d(x + iy)$.

Now to show the existence of division algorithm in G.

Let $\alpha \in G$ and let β be a non-zero element of G. Let $\alpha = x + iy$ and $\beta = m + in$. Define a complex number λ by the equation

$$\lambda = \frac{\alpha}{\beta} = \frac{x + iy}{m + in} = \frac{(x + iy)(m - in)}{m^2 + n^2} = p + iq,$$

where p, q are rational numbers.

Here λ is not necessarily a Gaussian integer.

Also division by β is possible since $\beta \neq 0$.

Let p' and q' be the nearest integers to p and q respectively.

Then obviously $|p - p'| \leq \frac{1}{2}$, $|q - q'| \leq \frac{1}{2}$.

Let $\lambda' = p' + iq'$. Then λ' is a Gaussian integer.

Now $\lambda = \frac{\alpha}{\beta} \Rightarrow \alpha = \lambda\beta \quad \Rightarrow \quad \alpha = \lambda'\beta + \lambda\beta - \lambda'\beta.$

Thus $\alpha = \lambda'\beta + (\lambda - \lambda')\beta.$...(1)

Since α, β, λ' are Gaussian integers, therefore from (1) it implies that $(\lambda - \lambda')\beta$ is also a Gaussian integer.

Now if p and q are integers then $p = p', q = q'$.

So $\lambda - \lambda' = (p - p') + i(q - q') = 0 + i0$. Thus $(\lambda - \lambda')\beta = 0 + i0$.

If p and q are not both integers, then $(\lambda - \lambda')\beta$ is a non-zero Gaussian integer and we have

$$d[(\lambda - \lambda')\beta] = d[\{(p - p') + i(q - q')\}(m + in)]$$

$$= [(p - p')^2 + (q - q')^2](m^2 + n^2) = [(p - p')^2 + (q - q')^2]\, d(\beta)$$

$$\leq \left[\frac{1}{4} + \frac{1}{4}\right] d(\beta) \qquad \left[\because (p - p')^2 \leq \frac{1}{4}, (q - q')^2 \leq \frac{1}{4}\right]$$

$$= \frac{1}{2} d(\beta) < d(\beta).$$

Thus $\alpha = \lambda'\beta + (\lambda - \lambda')\beta$, where λ' and $(\lambda - \lambda')\beta$ are Gaussian integers and either $(\lambda - \lambda')\beta = 0$

or $d[(\lambda - \lambda')\beta] < d(\beta)$.

Hence the ring of Gaussian integers is a Euclidean ring.

25 Properties of Euclidean Rings

Theorem 1: *Every Euclidean ring is a principal ideal ring.*

Proof: Let R be a Euclidean ring. Let S be an arbitrary ideal of R. If S is the null ideal, then $S = (0)$ *i.e.*, the ideal of R generated by 0. Therefore S is a principal ideal. So let us suppose that S is not a null ideal. Then there exist elements in S not equal to zero. Let b be a non-zero element in S such that $d(b)$ is minimum *i.e.*, there exists

no element c in S such that $d(c) < d(b)$. We shall show that $S = (b)$ *i.e.*, S is nothing but the ideal generated by b.

Let a be any element of S. Then by definition of Euclidean ring there exist elements q and r in R such that

$$a = qb + r \text{ where either } r = 0 \text{ or } d(r) < d(b).$$

Now $q \in R,\ b \in S \Rightarrow qb \in S$ because S is an ideal.

Further $a \in S,\ qb \in S \Rightarrow a - qb = r \in S.$

Thus $r \in S$ and we have either $r = 0$ or $d(r) < d(b)$.

If $r \neq 0$, then $d(r) < d(b)$ which contradicts our assumption that no element in S has d-value smaller than $d(b)$. Therefore we must have $r = 0$.

Then $a = qb.$

Thus every element a in S is a multiple of the generating element b. Thus $a \in S \Rightarrow a \in (b)$. Therefore $S \subseteq (b)$.

Again if xb is any element of (b), then $x \in R$.

Now $x \in R,\ b \in S \Rightarrow xb \in S.$ Therefore $(b) \subseteq S$.

Hence $S = (b)$.

Thus every ideal S in R is a principal ideal. Therefore R is a principal ideal ring.

Theorem 2: *Every Euclidean ring possesses unity element.*

Proof: Let R be a Euclidean ring. Obviously R is an ideal of R. Therefore there exists an element $u_0 \in R$ such that $R = (u_0)$ *i.e.*, there exists an element $u_0 \in R$ such that every element in R is a multiple of u_0. Since, in particular, $u_0 \in R$ therefore there exists an element $c \in R$ such that $u_0 = u_0 c$. We shall show that c is the required unity element. Let now a be any element of R. Since $a \in R$, therefore there exists some $x \in R$ such that $a = u_0\ x$.

Now
$$\begin{aligned} ac &= (u_0 x)\, c && [\because\ a = u_0 x] \\ &= (u_0 c)\, x && [\because\ R \text{ is a commutative ring}] \\ &= u_0 x && [\because\ u_0 = u_0 c] \\ &= a. && [\because\ a = u_0 x] \end{aligned}$$

Thus we have $ac = a = ca\ \ \forall\ \ a \in R.$

Hence c is the unity element.

Theorem3: *Let R be a Euclidean ring and a and b be any two elements in R, not both of which are zero. Then a and b have a greatest common divisor d which can be expressed in the form*

$$d = \lambda a + \mu b \text{ for some } \lambda, \mu \in R.$$

Proof: Consider the set

$$S = \{sa + tb \ :\ s, t \in R\}. \qquad \ldots(1)$$

We claim that S is an ideal of R. The proof is as follows :

Let $x = s_1 a + t_1 b$, and $y = s_2 a + t_2 b$ be any two elements of S.

Then $s_1, t_1, s_2, t_2 \in R$. We have

$$x - y = (s_1 a + t_1 b) - (s_2 a + t_2 b) = (s_1 - s_2) a + (t_1 - t_2) b \in S$$

since $s_1 - s_2$ and $t_1 - t_2$ are both elements of R.

Thus S is a subgroup of R with respect to addition.

Also if u be any element of R, then

$$xu = ux = u(s_1 a + t_1 b) = (us_1) a + (ut_1) b \in S \text{ since } us_1, ut_1 \in R.$$

Therefore S is an ideal of R. Now every ideal in R is a principal ideal. Therefore there exists an element d in S such that every element in S is a multiple of d.

Since $d \in S$, therefore from (1), we see that there exist elements $\lambda, \mu \in R$ such that

$$d = \lambda a + \mu b.$$

Now R is a ring with unity element 1.

$\therefore$ Putting $s = 1, t = 0$ in (1), we see that $a \in S$. Also putting $s = 0, t = 1$ in (1), we see that $b \in S$.

Now a, b are elements of S. Therefore they are both multiples of d. Hence $d \mid a$ and $d \mid b$.

Now suppose $c \mid a$ and $c \mid b$.

Then $c \mid \lambda a$ and $c \mid \mu b$. Therefore c is also a divisor of $\lambda a + \mu b$ *i.e.*, c is a divisor of d.

Thus d is a greatest common divisor of a and b.

Theorem 4: *Let a, b and c be any elements of a Euclidean ring R. Let* $(a, b) = 1$ *i.e., let the greatest common divisor of a and b be* 1. *If* $a \mid bc$, *then* $a \mid c$.

Proof: If the greatest common divisor of a and b is 1, then by theorem 3 there exist elements λ and μ in R such that

$$1 = \lambda a + \mu b. \qquad \ldots(1)$$

Multiplying both members of (1) by c, we get

$$c = \lambda ac + \mu bc. \qquad \ldots(2)$$

But $a \mid bc$, so there exists an element $q \in R$ such that $bc = qa$.

Substituting this value of bc in (2), we get

$$c = \lambda ac + \mu qa = (\lambda c + \mu q) a,$$

which shows that a is a divisor of c. Hence the theorem.

Theorem 5: *If p is a prime element in the Euclidean ring R and* $p \mid ab$ *where* $a, b \in R$ *then p divides at least one of a or b.*

Proof: If p divides a, we are nothing to prove. So suppose that p does not divide a. Since p is prime and p does not divide a, therefore p and a are relatively prime *i.e.*, the greatest common divisor of p and a is 1. Hence by theorem 4, we get that $p \mid b$.

Corollary: *If p is a prime element in the Euclidean ring R and p divides the product*

$a_1\ a_2\ \ldots\ a_n$ of elements in R , then p divides at least one of $a_1, a_2, \ldots, a_n$.
The result follows immediately by repeated application of theorem 5.

Theorem 6: *Let R be a Euclidean ring. Let a and b be two non-zero elements in R. Then*

(*i*) *if b is a unit in R, d (ab) = d (a).*

(*ii*) *if b is not a unit in R, d (ab) > d (a).*

Proof: (i) By the definition of Euclidean ring, we have

$$d\,(ab) \geq d\,(a). \qquad \ldots(1)$$

Now suppose that b is a unit in R. Then b is inversible and b^{-1} exists. We can write

$$a = (ab)\,b^{-1}.$$

$$\therefore \quad d\,(a) = d\,[(ab)\,b^{-1}].$$

But by the definition of Euclidean ring, we have

$$d\,[(ab)\,b^{-1}] \geq d\,(ab).$$

$$\therefore \quad d\,(a) \geq d\,(ab). \qquad \ldots(2)$$

From (1) and (2), we conclude that

$$d\,(ab) = d\,(a).$$

(ii) Suppose now that b is not a unit in R. Since a and b are non-zero elements of the Euclidean ring R, therefore ab is also a non-zero element of R. Now $a \in R$ and $0 \neq ab \in R$, therefore by definition of Euclidean ring there exist elements q and r in R such that

$$a = q(ab) + r \qquad \ldots(3)$$

where either $r = 0$ or $d\,(r) < d\,(ab)$.

If $r = 0$, then

$$a = qab \quad \Rightarrow \quad a - qab = 0 \quad \Rightarrow \quad a(1 - qb) = 0$$

$$\Rightarrow \quad 1 - qb = 0 \qquad [\because\ a \neq 0 \text{ and } R \text{ is free of zero divisors}]$$

$$\Rightarrow \quad qb = 1 \Rightarrow b \text{ is inversible } \Rightarrow b \text{ is a unit in } R.$$

Thus we get a contradiction. Hence r cannot be zero. Therefore we must have

$$d\,(r) < d\,(ab) \quad i.e., \quad d\,(ab) > d\,(r). \qquad \ldots(4)$$

Also from (3), we have

$$r = a - qab = a\,(1 - qb).$$

$$\therefore \quad d\,(r) = d\,[a(1 - qb)].$$

But $\quad d\,[a(1 - qb)] \geq d\,(a).$

$$\therefore \quad d\,(r) \geq d\,(a). \qquad \ldots(5)$$

From (4) and (5), we conclude that $d\,(ab) > d\,(a)$.

Theorem 7: *The necessary and sufficient condition that the non-zero element a in the Euclidean ring R is a unit is that*

$$d\,(a) = d\,(1). \qquad \textbf{(Lucknow 2011)}$$

Proof: Let a be a unit in R. Then to prove that $d(a) = d(1)$.

By the definition of Euclidean ring

$$d(1a) \geq d(1) \quad \Rightarrow \quad d(a) \geq d(1). \qquad ...(1)$$

Since a is a unit in R, therefore a^{-1} exists and we have

$$1 = aa^{-1} \quad \Rightarrow \quad d(1) = d(aa^{-1}).$$

But $d(aa^{-1}) \geq d(a)$.

$\therefore$ $d(1) \geq d(a)$. ...(2)

From (1) and (2), we conclude that $d(a) = d(1)$.

Conversely let $d(a) = d(1)$. Then to prove that a is a unit in R. If a is not a unit in R, then by theorem 6, we have

$$d(1a) > d(1) \quad \Rightarrow \quad d(a) > d(1).$$

Thus we get a contradiction. Hence a must be a unit in R.

Theorem 8: *Let R be a Euclidean ring. Then every non-zero element in R is either a unit in R or can be written as a product of a finite number of prime elements of R.*

Proof: Let a be a non-zero element of R. We are to prove that either a is a unit in R or it can be written as a product of a finite number of prime elements of R. We shall prove the result by induction on $d(a)$ *i.e.*, by induction on the d- value of a.

Let us first start the induction. We have $a = 1a$. Therefore $d(a) \geq d(1)$. Thus 1 is an element in R which has the minimal d - value. If $d(a) = d(1)$, then a is a unit in R. [See theorem 7]. Thus the result of the theorem is true if $d(a) = d(1)$ and so we have started the induction.

Now assume as our induction hypothesis that the theorem is true for all non-zero elements $x \in R$ such that $d(x) < d(a)$. Then we shall show that the theorem is true for a also. If a is a prime element of R, the theorem is obviously true. So suppose that a is not prime. Then we can write $a = bc$ where neither b nor c is a unit in R. Since both b and c are not units in R, therefore $d(bc) > d(b)$ and $d(bc) > d(c)$. But $d(a) = d(bc)$. Therefore we have $d(b) < d(a)$ and $d(c) < d(a)$. So by our induction hypothesis each of b and c can be written as a product of a finite number of prime elements of R.

Let $b = p_1 p_2 \ldots p_n$, $c = q_1 q_2$ where the p's and q's are prime elements of R.

Then $a = bc = p_1 p_2 \ldots p_n q_1 q_2 \ldots q_m$.

Thus we have written a as a product of a finite number of prime elements of R. This completes the induction and so the theorem has been proved.

Theorem 9: Unique Factorization theorem: *Let R be a Euclidean ring and a be a non-zero non-unit element in R. Suppose that*

$$a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$$

where the p's and q's are prime elements of R. Then $m = n$ and each p is an associate of some q and each q is an associate of some p.

Proof: We have $p_1\ p_2 \ldots p_m = q_1\ q_2 \ldots q_n$. Now p_1 is a divisor of $p_1\ p_2 \ldots p_m$. Therefore p_1 is also a divisor of $q_1\ q_2 \ldots q_n$. By Corollary to Theorem 5, p_1 must divide at least one of $q_1, q_2, \ldots, q_n$. Since R is a commutative ring, therefore without loss of generality we may suppose that p_1 divides q_1. But p_1 and q_1 are both prime elements in R. Therefore p_1 and q_1 must be associates and we have $q_1 = up_1$ where u is a unit in R. Thus we have

$$p_1\ p_2 \ldots p_m = up_1\ q_2 \ldots q_n.$$

Cancelling $0 \neq p_1$ from both sides, we get

$$p_2\ p_3 \ldots p_m = uq_2\ q_3 \ldots q_n. \qquad \ldots(1)$$

Now we can repeat the above argument on the relation (1) with p_2. If $n > m$, then after m steps the left hand side becomes 1 while the right hand side reduces to a product of some units in R and certain number of q's (the excess of n over m). But the q's are prime elements of R and so they are not units in R. So the product of some units in R and certain number of q's cannot be equal to 1. Therefore n cannot be greater than m.

Thus $n \leq m$.

Similarly interchanging the roles of p's and q's we get $m \leq n$.

Hence $m = n$.

Also in the above process we have shown that every p is an associate of some q and conversely every q is an associate of some p. Hence the theorem has been completely established.

Note: Combining theorems 8 and 9, we can say that *every non-zero element in a Euclidean ring R can be uniquely written (upto associates) as a product of prime elements or is a unit in R . Therefore a Euclidean ring is a Unique Factorization Domain.*

Theorem 10: *An ideal S of the Euclidean ring R is maximal iff S is generated by some prime element of R .*

Proof: We know that every ideal of a Euclidean ring R is a principal ideal. Suppose S is an ideal of R generated by p so that $S = (p)$. Now we are to prove that

(i) S is maximal if p is a prime element of R.

(ii) p is prime if S is maximal.

First we shall prove (i). Let p be a prime element of R such that $(p) = S$. Let T be an ideal of R such that $S \subseteq T \subseteq R$. Since T is also a principal ideal of R, so let $T = (q)$ where $q \in R$.

Now $S \subseteq T \Rightarrow (p) \subseteq (q) \Rightarrow p \in (q)$

$\Rightarrow$ $p = xq$ for some $x \in R \Rightarrow q \mid p$.

Since p is prime, therefore either q should be a unit in R or q should be an associate of p.

If q is a unit in R, then

$$T = (q) = R.$$

If q is an associate of p, then

$$T = (q) = (p) = S.$$

Thus either $T = R$ or $T = S$.

Now we shall prove (ii). Let $(p) = S$ be a maximal ideal. We are to show that p is prime. Let us suppose that p is composite *i.e.*, p is not prime.

Let $p = mn$ where neither m nor n is a unit in R.

Now $p = mn \Rightarrow m \mid p \quad \Rightarrow \quad (p) \subseteq (m)$.

But $(m) \subseteq R$. Therefore we have

$$(p) \subseteq (m) \subseteq R.$$

But (p) is a maximal ideal, therefore we should have either

$$(m) = (p) \text{ or } (m) = R.$$

If $R = (m)$, then $R \subseteq (m)$.

$\therefore \quad 1 \in R \Rightarrow 1 \in (m) \quad \Rightarrow \quad 1 = ym$ for some $y \in R$

$\Rightarrow \quad m$ is inversible $\quad \Rightarrow \quad m$ is a unit in R.

Thus we get a contradiction.

If $(m) = (p)$, then $m \in (p)$. Therefore $m = lp$ for some $l \in R$.

$\therefore \quad p = mn = lpn = pln.$

$\therefore \quad p(1 - ln) = 0$

$\Rightarrow \quad 1 - ln = 0 \qquad [\because p \neq 0$ and R is without zero divisors$]$

$\Rightarrow \quad ln = 1 \Rightarrow n$ is inversible

$\Rightarrow \quad n$ is a unit in R.

This is again a contradiction. Hence p must be a prime element of R.

26 Polynomial Rings over Unique Factorization Domains

We have already defined a unique factorization domain. For the sake of convenience we repeat the definition here.

Unique Factorization Domain: Definition: *An integral domain R, with unity element 1 is a unique factorization domain if*

(*a*) *any non-zero element in R is either a unit or can be written as the product of a finite number of irreducible (prime) elements of R.*

(*b*) *the decomposition in part (a) is unique upto the order and associates of the irreducible elements.*

In general commutative rings we have defined the greatest common divisors of elements. But the difficulty is that in an arbitrary commutative ring these might not exist. However, in unique factorization domain their existence is assured. Further we know that in an integral domain with unity in case a greatest common divisor of some elements exists, it is unique apart from the distinction between associates.

Theorem 1: *Let R be a unique factorization domain and a and b be any two elements in R, not both of which are zero. Then a and b have a greatest common divisor (a, b) in R. Moreover, if a and b are relatively prime (i.e., (a, b) is a unit in R), then* $a \mid bc \Rightarrow a \mid c$.

Proof: Suppose a and b are any two elements, not both of which are zero, of a unique factorization domain R. If one of a and b, say, b is 0, then obviously a is the greatest common divisor of a and b. If any of a and b, say a, is a unit in R, then obviously a is the greatest common divisor of a and b. So let us suppose that neither $a = 0$ nor $b = 0$ and none of these is a unit in R. Then each of a and b can be uniquely expressed as the product of a finite number of irreducible elements of R.

Let $$a = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}, \quad \dots(1)$$

and $$b = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}, \quad \dots(2)$$

where we have arranged the expressions in such a way that the same irreducible factors $p_1, p_2, \dots, p_r$ appear in both. Note that we can definitely do so because the integer 0 can be used as power in any case, if necessary. The elements $p_1, p_2, \dots, p_r$ are all different primes and $m_1, m_2, \dots, m_r, n_1, n_2, \dots, n_r$ are all integers ≥ 0.

Let g_i = minimum (m_i, n_i), where $i = 1, 2, \dots, r$. Then obviously

$$p_1^{g_1} p_2^{g_2} \dots p_r^{g_r}$$

is the greatest common divisor of a and b.

This proves the existence of greatest common divisor.

Now suppose that a and b are relatively prime *i.e.,* the greatest common divisor of a and b is a unit in R. Also suppose that

$$a \mid bc.$$

If a is a unit in R, then obviously a is a divisor of c. So let a be not a unit in R. Then a can be uniquely expressed as the product of a finite number of prime elements of R.

Let $$a = q_1 q_2 \dots q_s,$$

where $q_1, q_2, \dots, q_s$ are prime elements of R.

We have $a \mid bc \Rightarrow bc = ka$ for some $k \in R$

$$\Rightarrow \quad bc = kq_1 q_2 \dots q_s. \quad \dots(3)$$

Since each element of R can be uniquely expressed as the product of a finite number of prime elements of R, therefore each of the prime elements $q_1, q_2, \dots, q_s$ must occur as a factor of either b or c. But none of $q_1, q_2, \dots, q_s$ can be a factor of b because otherwise a and b will not remain relatively prime. Therefore each of $q_1, q_2, \dots, q_s$ must be a factor of c. Hence

$$q_1 q_2 \dots q_s \text{ is a divisor of } c \Rightarrow a \mid c.$$

Note: In a similar manner we can prove that if $a_1, \dots, a_n$ are any n elements of a unique factorization domain, they possess a greatest common divisor which will be unique apart from the distinction between associates. Thus if g_1, g_2 are two greatest common divisors of these n elements, then by the definition of greatest common divisor, we have

$g_1 \mid g_2$ and $g_2 \mid g_1$

$\Rightarrow$ g_1 and g_2 are associates

$\Rightarrow$ $g_1 = u g_2$ where u is a unit in R.

Thus the greatest common divisor of some elements is unique within units of R.

Theorem 2: *If a is a prime element of a unique factorization domain R and b, c are any elements of R, then*

$$a \mid bc \Rightarrow a \mid b \text{ or } a \mid c.$$

Proof: If $a \mid b$, then obviously the theorem is proved. So let a be not a divisor of b. Since a is a prime element of R and a is not a divisor of b, therefore we claim that a and b are relatively prime. Since a is a prime element of R, therefore the only divisors of a are the associates of a or the units of R. Now an associate of a cannot be a divisor of b otherwise a itself will be a divisor of b while we have assumed that a is not a divisor of b. Thus the units of R are the only divisors of a which also divide b. Therefore the greatest common divisor of a and b is a unit of R.

Since a and b are relatively prime, therefore by theorem 1, we have

$$a \mid bc \Rightarrow a \mid c.$$

This completes the proof of the theorem.

27 Polynomial Rings over Unique Factorization Domains

Let R be a unique factorization domain. Since R is an integral domain with unity, therefore $R[x]$ is also an integral domain with unity. Also any unit, (inversible element) in $R[x]$ must already be a unit in R. Thus the only units in $R[x]$ are the units of R. A polynomial $p(x) \in R[x]$ is *irreducible* over R *i.e.,* irreducible as an element of $R[x]$ if whenever $p(x) = a(x)\, b(x)$ with $a(x), b(x) \in R[x]$, then one of $a(x)$ or $b(x)$ is a unit in $R[x]$ *i.e.,* a unit in R.

For example: If $\mathbf{I}$ is the ring of integers, then $\mathbf{I}$ is a unique factorization domain. The polynomial $2x^2 + 4 \in \mathbf{I}[x]$ is a reducible element of $\mathbf{I}[x]$. We have $2x^2 + 4 = 2(x^2 + 2)$. Neither 2 nor $x^2 + 2$ is a unit in $\mathbf{I}[x]$. On the other hand the polynomial $x^2 + 1 \in \mathbf{I}[x]$ is an irreducible element of $\mathbf{I}[x]$.

28 Content of a Polynomial

Definition: *Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ be a polynomial over a unique factorization domain R. Then the content of $f(x)$ denoted by $c(f)$, is defined as the greatest common divisor of the coefficients $a_0, a_1, \ldots, a_n$ of $f(x)$. Obviously the content of $f(x)$ is unique within units of R. Thus if c_1 and c_2 are two contents of $f(x)$, then we must have $c_1 = u c_2$ where u is some unit in R.*

29 Primitive Polynomial

Definition: *Let R be a unique factorization domain. Then a polynomial $f(x) = a_0 + a_1 x + ... + a_n x^n \in R[x]$ is said to be primitive if the greatest common divisor of its coefficients $a_0, a_1, \ldots, a_n$ is a unit in R.* Thus a polynomial $f(x)$ is primitive if its content is 1 (that is a unit in R). If

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

is a monic polynomial over R, then obviously $f(x)$ is primitive.

If $\mathbf{I}$ is the ring of integers, then $3x^3 - 5x^2 + 7$ is a primitive member of $\mathbf{I}[x]$ while $2x^2 - 4x + 8$ is not a primitive member of $\mathbf{I}[x]$.

Every irreducible polynomial of positive degree belonging to $R[x]$ is necessarily primitive. But an irreducible polynomial of zero degree may not be primitive. For example $3 \in \mathbf{I}[x]$ is irreducible but it is not primitive. Further a primitive polynomial may not be irreducible. For example $x^2 + 5x + 6 \in \mathbf{I}[x]$ is primitive and it is not irreducible. We have

$$x^2 + 5x + 6 = (x + 2)(x + 3).$$

Theorem 1: *Let R be a unique factorization domain. Prove that every non-zero member $f(x)$ of $R[x]$ can be written as $f(x) = g f_1(x)$ where $g = c(f)$ and where $f_1(x)$ is primitive. Also prove that this decomposition of $f(x)$ as an element of R by a primitive polynomial in $R[x]$ is unique apart from the distinction between associates.*

Proof: Let R be a unique factorization domain and let

$$f(x) = a_0 + a_1 x + ... + a_n x^n \in R[x].$$

Since R is a unique factorization domain, therefore the elements $a_0, a_1, \ldots, a_n \in R$ must possess a greatest common divisor. Let $g \in R$ be the greatest common divisor of these elements. Then $g = c(f)$. Let

$$a_i = g b_i \text{ where } i = 0, 1, \ldots, n.$$

Then $$f(x) = g b_0 + g b_1 x + ... + g b_n x^n = g[b_0 + b_1 x + \ldots + b_n x^n].$$

Since g is the greatest common divisor of $a_0, a_1, \ldots, a_n$, therefore the elements $b_0, b_1, \ldots, b_n$ can have no common factor other than units of R. Consequently the polynomial

$$f_1(x) = b_0 + b_1 x + \ldots + b_n x^n$$

is a primitive member of $R[x]$. Thus we have $f(x) = g f_1(x)$, where $g \in R$ and $f_1(x) \in R[x]$ is primitive.

Now we come to the uniqueness part of the theorem.

If possible, let

$$f(x) = h f_2(x) \text{ where } h \in R \text{ and } f_2(x) \in R[x] \text{ is primitive.}$$

Then $g f_1(x) = h f_2(x)$...(1)

Since $f_1(x)$ and $f_2(x)$ are both primitive, therefore the content of the polynomial on the left hand side of (1) is g and the content of the polynomial on the right hand side of (1) is h. But the content of a polynomial is unique upto associates. Therefore g and h are associates

$\Rightarrow$ $g = hu$ where u is some unit in R

$\Rightarrow$ $hu\ f_1(x) = h f_2(x)$

$\Rightarrow$ $u f_1(x) = f_2(x)$ [by left cancellation law in the integral domain $R[x]$, since $h \neq 0$]

$\Rightarrow$ $f_1(x)$ and $f_2(x)$ are associates.

Hence the theorem.

Theorem 2: *If R is a unique factorization domain, then the product of two primitive polynomials in $R[x]$ is again a primitive polynomial in $R[x]$.*

Proof: Let

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \text{and} \quad g(x) = b_0 + b_1 x + \ldots + b_m x^m$$

be two primitive polynomials in $R[x]$.

Let $h(x) = f(x)\ g(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$.

Suppose $h(x)$ is not primitive. Then all the coefficients of $h(x)$ must be divisible by some prime element p of R. Since $f(x)$ is primitive, therefore the prime element p must not divide some coefficient of $f(x)$. Let a_i be the first coefficient of $f(x)$ which p does not divide. Similarly let b_j be the first coefficient of $g(x)$ which p does not divide. In $f(x)\ g(x)$, the coefficient of x^{i+j} is

$$c_{i+j} = a_i b_j + (a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots + a_0 b_{i+j}) + (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0)$$

From this relation, we get

$$a_i b_j = c_{i+j} - (a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots + a_0 b_{i+j}) - (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0) \quad \ldots(1)$$

Now by our choice of a_i, p is a divisor of each of the elements $a_0, a_1, \ldots, a_{i-1}$.

Therefore $p \mid (a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \ldots + a_0 b_{i+j})$.

Similarly, by our choice of b_j, p is a divisor of each of the elements $b_0, b_1, \ldots, b_{j-1}$. Therefore

$$p \mid (a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \ldots + a_{i+j} b_0).$$

Also by assumption $p \mid c_{i+j}$.

Hence from (1), we get

$$p \mid a_i b_j \quad \Rightarrow \quad p \mid a_i \text{ or } p \mid b_j, \text{ since } p \text{ is a prime element of } R.$$

But this is nonsense because according to our assumption p is not a divisor of a_i and also p is not a divisor of b_j.

Hence $h(x)$ must be primitive. This proves the theorem.

Theorem 3: *If R is a unique factorization domain and if $f(x)$, $g(x)$ are in $R[x]$, then*

$$c(fg) = c(f)\, c(g) \text{ (upto units)}.$$

Proof: The polynomial $f(x)$ in $R[x]$ can be written as $f(x) = a f_1(x)$, where $a = c(f)$ and $f_1(x)$ is primitive. Similarly the polynomial $g(x)$ can be written as $g(x) = b\, g_1(x)$, where $b = c(g)$ and $g_1(x)$ is primitive. Then

$$f(x)\ g(x) = ab\, f_1(x)\ g_1(x). \qquad \ldots(1)$$

Since $f_1(x)$ and $g_1(x)$ are both primitive, therefore $f_1(x)\ g_1(x)$ is also primitive. [Refer theorem 2].

Therefore from (1), we see that the content of $f(x)\ g(x)$ is either ab or some associate of ab. Thus the content of $f(x)\ g(x)$ is ab (upto units). Therefore

$$c(fg) = ab = c(f)\, c(g).$$

This proves the theorem.

30 Field of Quotients of a Unique Factorization Domain

If R is a unique factorization domain, then R is necessarily an integral domain. Therefore R has a field of quotients. Throughout this section we shall denote the field of quotients of R by F. We can consider $R[x]$ to be a subring of $F[x]$.

Theorem 1: *If R is an integral domain (not necessarily a unique factorization domain) and F is its field of quotients, then any element $f(x)$ in $F[x]$ can be written as*

$$f(x) = \frac{f_0(x)}{a},$$

where $f_0(x) \in R[x]$ and where $a \in R$.

Proof: Let F be the field of quotients of an integral domain R. Then

$$F = \left\{ \frac{p}{q} : p \in R, 0 \neq q \in R \right\}.$$

Let $f(x)$ be an element of $F[x]$. Let

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \ldots. + \frac{a_n}{b_n} x^n, \text{ where } a_0, a_1, \ldots, a_n \in R$$

and $b_0, b_1, \ldots, b_n$ are non-zero elements of R.

Now $b_0, b_1, \ldots, b_n$ are also non-zero elements of F. So each of them must be inversible. Further $b_0\ b_1 \ldots b_n$ is also a non-zero element of F and so it is also inversible. Then we can write

$$f(x) = \frac{b_0\ b_1 \ldots b_n}{b_0\ b_1 \ldots b_n} \left(\frac{a_0}{b_0} + \frac{a_1}{b_1} x + \ldots. + \frac{a_n}{b_n} x^n \right)$$

$$= \frac{(a_0\ b_1 b_2 \ldots b_n) + (b_0\ a_1 b_2 \ldots b_n)\, x + \ldots + (b_0\ b_1 \ldots b_{n-1}\ a_n)\, x^n}{b_0\ b_1 \ldots b_n}$$

$$= \frac{f_0(x)}{a},$$

where obviously

$$f_0(x) = (a_0 b_1 b_2 \ldots b_n) + (b_0\ a_1 b_2 \ldots b_n)\ x + \ldots + (b_0\ b_1 \ldots b_{n-1}\ a_n)\ x^n$$

is in $R[x]$ and $a = b_0 b_1 \ldots b_n$ is in R.

Theorem 2: (Gauss' Lemma): *Let F be the field of quotients of a unique factorization domain R . If the primitive polynomial $f(x) \in R[x]$ can be factored as the product of two polynomials having coefficients in F, then it can be factored as the product of two polynomials having coefficients in R.*

Proof: Let R be a unique factorization domain and F be its field of quotients. Let $f(x) \in R[x]$ be primitive.

Let $f(x) = g(x)\ h(x)$ where $g(x)$ and $h(x)$ have coefficients in F.

Since $g(x), h(x) \in F[x]$, therefore we can write

$$g(x) = \frac{g_0(x)}{a},\ h(x) = \frac{h_0(x)}{b},$$

where $a, b \in R$ and where $g_0(x), h_0(x) \in R[x]$.

Also $g_0(x) = \alpha\ g_1(x),\ h_0(x) = \beta\ h_1(x)$,

where $\alpha = c(g_0),\ \beta = c(h_0)$ and where $g_1(x), h_1(x)$ are primitive members of $R[x]$. [See theorem 1 of article 29.]

Thus $$f(x) = \frac{\alpha\beta}{ab}\ g_1(x)\ h_1(x)$$

$$\Rightarrow \quad ab\ f(x) = \alpha\beta\ g_1(x)\ h_1(x). \qquad \ldots(1)$$

Since $g_1(x)$ and $h_1(x)$ are both primitive members of $R[x]$, therefore $g_1(x)\ h_1(x)$ is also a primitive member of $R[x]$. Therefore from (1), we conclude that $f(x)$ and $g_1(x)\ h_1(x)$ are associates in $R[x]$. (See theorem 1 of article 29). Thus

$$f(x) = u g_1(x)\ h_1(x) \text{ where } u \text{ is a unit in } R[x] \text{ and so a unit of } R.$$

Now $u \in R,\ g_1(x) \in R[x] \Rightarrow u g_1(x)$ is a member of $R[x]$. Also $h_1(x)$ is a member of $R[x]$. Hence $f(x)$ can be factored as the product of two polynomials with coefficients in R.

Note: Let **I** be the ring of integers. Then **I** is a Euclidean ring and so a unique factorization domain. The field of quotients of **I** is the field of rational numbers. If in the above theorem we take **I** in place of R, then the statement of the theorem is as follows :

If the primitive polynomial $f(x) \in \mathbf{I}[x]$ can be factored as the product of two polynomials having rational coefficients it can be factored as the product of two polynomials having integer coefficients.

For its proof simply replace R by **I** or say, 'let R be the ring of integers'.

Theorem 3: *Let F be the field of quotients of a unique factorization domain R. If $f(x) \in R[x]$ is both primitive and irreducible as an element of $R[x]$, then it is irreducible as an element of $F[x]$. Conversely, if the primitive element $f(x)$ in $R[x]$ is irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$.*

Proof: Let $f(x)$ be a primitive member of $R[x]$. Suppose $f(x)$ is irreducible in $R[x]$ but is reducible in $F[x]$. Since F is a field and $f(x)$ is reducible in $F[x]$, therefore we must have $f(x) = g(x)\, h(x)$, where $g(x), h(x)$ are in $F[x]$ and are of positive degree. Now we can write

$$g(x) = \frac{g_0(x)}{a}, h(x) = \frac{h_0(x)}{b},$$

where $a, b \in R$, and where $g_0(x), h_0(x) \in R[x]$.

Also $g_0(x) = \alpha\, g_1(x), h_0(x) = \beta\, h_1(x)$

where $\alpha = c(g_0)$, $\beta = c(h_0)$, and where $g_1(x), h_1(x)$ are primitive members of $R[x]$. [See theorem 1 of article 29].

Thus $$f(x) = \frac{\alpha\beta}{ab}\, g_1(x)\, h_1(x)$$

$$\Rightarrow \quad ab\, f(x) = \alpha\beta\, g_1(x)\, h_1(x). \qquad \ldots(1)$$

Since $g_1(x)$ and $h_1(x)$ are both primitive members of $R[x]$, therefore $g_1(x)\, h_1(x)$ is also a primitive member of $R[x]$. Therefore from (1), we conclude that $f(x)$ and $g_1(x)\, h_1(x)$ are associates in $R[x]$. [See theorem 1 of article 29].

Thus $f(x) = ug_1(x)\, h_1(x)$ where u is a unit in $R[x]$ and so a unit in R.

Let $ug_1(x) = g_2(x)$. Then

$$f(x) = g_2(x)\, h_1(x), \text{ where } g_2(x), h_1(x) \in R[x].$$

We have deg $g_2(x) =$ deg $g(x)$, and deg $h_1(x) =$ deg $h(x)$.

Thus deg $g_2(x) > 0$, deg $h_1(x) > 0$.

Therefore neither $g_2(x)$ nor $h_1(x)$ is a unit in $R[x]$.

Thus $f(x) = g_2(x)\, h_1(x)$ is a proper factorization of $f(x)$ in $R[x]$. This contradicts the given statement that $f(x)$ is irreducible in $R[x]$. Hence $f(x)$ must be irreducible in $F[x]$.

Converse: Suppose $f(x)$ is a primitive member of $R[x]$ and is irreducible as an element of $F[x]$. Then to prove that $f(x)$ is also irreducible as an element of $R[x]$.

Let $$f(x) = g(x)\, h(x), \text{ where } g(x), h(x) \in R[x].$$

Then $f(x)$ will be irreducible in $R[x]$ if one of $g(x)$ or $h(x)$ is a unit in $R[x]$ *i.e.,* a unit in R.

Now $g(x), h(x) \in R[x]$ can also be treated as $g(x), h(x) \in F[x]$.

Since $f(x)$ is irreducible as an element of $F[x]$, therefore one of $g(x)$ or $h(x)$ must be of degree 0. Suppose deg $g(x) = 0$. Then $g(x)$ is a constant polynomial.

Let $g(x) = k \in R$. Then

$$f(x) = kh(x).$$

Now $f(x)$ is a primitive member of $R[x]$. Therefore $c(f)$ is a unit in R. If k is not a unit in R, then content of $kh(x)$ cannot be a unit in R and so it cannot be equal to $c(f)$. Hence k must be a unit in R. Consequently $f(x)$ is irreducible as an element of $R[x]$.

This completes the proof of the theorem.

Theorem 4: *Let F be the field of quotients of a unique factorization domain R. If $f_1(x)$, $f_2(x)$ are two primitive members of $R[x]$ and are associates in $F[x]$, then they are also associates in $R[x]$.*

Proof: Since $f_1(x)$, $f_2(x)$ are associates in $F[x]$, therefore we have

$$f_1(x) = k\ f_2(x) \text{ where } 0 \neq k \in F$$

i.e., k is a unit in $F[x]$.

Note that the only units of $F[x]$ are the non-zero elements of F.

Now F is the field of quotients of R. Therefore

$$0 \neq k \in F \ \Rightarrow\ k = \frac{g}{h} \text{ where } g, 0 \neq h \in R.$$

$$\therefore \qquad f_1(x) = \frac{g}{h} f_2(x) \qquad \Rightarrow \qquad h f_1(x) = g\ f_2(x).$$

Since $h, g \in R$ and $f_1(x)$, $f_2(x)$ are primitive members of $R[x]$, therefore by theorem 1 of article 8, $f_1(x)$ and $f_2(x)$ are associates in $R[x]$.

Theorem 5: *If R is a unique factorization domain and if $p(x)$ is a primitive polynomial in $R[x]$, then it can be factored in a unique way as the product of irreducible elements in $R[x]$. Hence show that the polynomial ring $R[x]$ over a unique factorization domain R is itself a unique factorization domain.*

Proof: Let F be the field of quotients of a unique factorization domain R. Let $p(x)$ be a primitive member of $R[x]$. We can regard $p(x)$ as a member of $F[x]$. Since F is a field, therefore $F[x]$ is a unique factorization domain. Recall that the ring of polynomials over a field is a unique factorization domain. Therefore $p(x) \in F[x]$ can be factored as

$$p(x) = p_1(x)\ p_2(x) \ldots p_k(x),$$

where $p_1(x), p_2(x), \ldots, p_k(x)$ are irreducible polynomials in $F[x]$. Now each $p_i(x)$, $1 \leq i \leq k$, can be written as $p_i(x) = \frac{f_i(x)}{a_i}$, where $a_i \in R$ and $f_i(x) \in R[x]$. Further $f_i(x)$ can be written as

$$f_i(x) = c_i\ q_i(x),$$

where $c_i \in R$ and $q_i(x)$ is a primitive member of $R[x]$. Thus each $p_i(x) = \frac{c_i}{a_i} q_i(x)$,

where $c_i, a_i \in R$ and $q_i(x)$ is a primitive member of $R[x]$. Since $p_i(x)$ is irreducible in $F[x]$, therefore $q_i(x)$ must also be irreducible in $F[x]$. Now $q_i(x)$ is a primitive member of $R[x]$ and $q_i(x)$ is irreducible in $F[x]$. Therefore, by converse part of theorem 3, $q_i(x)$ is irreducible in $R[x]$.

Now $$p(x) = p_1(x)\ p_2(x) \ldots p_k(x)$$

$$= \frac{c_1 c_2 \ldots c_k}{a_1 a_2 \ldots a_k} q_1(x)\, q_2(x) \ldots q_k(x).$$

$$\therefore \quad a_1 a_2 \ldots a_k\ p(x) = c_1\ c_2\ \ldots c_k\ q_1(x)\, q_2(x) \ldots q_k(x). \qquad \ldots(1)$$

Since $q_1(x), \ldots, q_k(x)$ are all primitive members of $R[x]$, therefore

$$q_1(x)\, q_2(x) \ldots q_k(x)$$

is also a primitive member of $R[x]$. Further $p(x)$ is primitive.

Therefore from the relation (1), we conclude with the help of theorem 1 of article 29 that $p(x)$ and $q_1(x)\, q_2(x) \ldots q_k(x)$ are associates in $R[x]$. Therefore

$$p(x) = u\, q_1(x)\, q_2(x) \ldots q_k(x)$$

where u is some unit in $R[x]$ and hence in R.

If $q_1(x)$ is irreducible in $R[x]$ then $u\, q_1(x)$ is also irreducible in $R[x]$. If we simply replace $u\, q_1(x)$ by $q_1(x)$, then we get

$$p(x) = q_1(x)\, q_2(x) \ldots q_k(x).$$

Thus we have factored $p(x)$ in $R[x]$ as a product of irreducible elements.

Now to show that the above factorization of $p(x)$ is unique upto the order and associates of irreducible elements.

Let $p(x) = r_1(x)\, r_2(x) \ldots r_m(x)$, where the $r_i(x)$ are irreducible in $R[x]$. Since $p(x)$ is primitive, therefore each $r_i(x)$ must be primitive. Consequently by theorem 3, each $r_i(x)$ must be irreducible in $F[x]$. But $F[x]$ is a unique factorization domain. Therefore $p(x) \in F[x]$ can be uniquely expressed as the product of irreducible elements of $F[x]$. Hence the $r_i(x)$ and the $q_i(x)$ regarded as the elements of $F[x]$ are equal (upto associates) in some order.

Since $r_i(x)$ and $q_i(x)$ are primitive members of $R[x]$ and are associates in $F[x]$, therefore by theorem 4, they are also associates in $R[x]$. Thus $p(x)$ has a unique factorization as a product of irreducible elements of $R[x]$.

Now we are in a position to prove that if R is a unique factorization domain, then so is $R[x]$.

Let $f(x) \in R[x]$ be arbitrary. Then we can write $f(x)$ in a unique way as $f(x) = c\, g(x)$ where $c \in R$ and $g(x)$ is a primitive member of $R[x]$.

Now by the above discussion $g(x)$ can be uniquely expressed as the product of irreducible elements of $R[x]$. What about c ?

Let $\quad c = h_1(x)\, h_2(x) \ldots h_s(x)$, where $h_1(x), \ldots, h_s(x) \in R[x]$.

We have $0 = \deg c = \deg h_1(x) + \deg h_2(x) + \ldots + \deg h_s(x)$

$\Rightarrow$ each $h_i(x)$ must be of degree 0

$\Rightarrow$ each $h_i(x)$ is an element of R.

Thus the only factorization of c as an element of $R[x]$ are those it had as an element of R. In particular if $\alpha \in R$ is irreducible, then $\alpha \in R[x]$ is also irreducible. But R is a unique factorization domain. Therefore $c \in R$ can be uniquely expressed as the product of irreducible elements of R and hence of $R[x]$.

Finally, we conclude that $f(x) = c\, g(x)$ can be uniquely expressed as the product of irreducible elements of $R[x]$. Hence $R[x]$ is a unique factorization domain.

Corollary 1: *If R is a unique factorization domain then so is $R[x_1, \ldots, x_n]$.*

Proof: If R is a unique factorization domain, then we know that $R_1 = R[x_1]$ is a unique factorization domain. Now R_1 is a unique factorization domain implies that

$$R_2 = R_1[x_2] = R[x_1, x_2]$$

is a unique factorization domain. Continuing this process a finite number of times we conclude that $R[x_1, \ldots, x_n]$ is a unique factorization domain.

Corollary 2: *If F is a field, then $F[x_1, x_2, \ldots, x_n]$ is a unique factorization domain.*

Proof: If F is a field, then we know that $F_1 = F[x_1]$ is a unique factorization domain. Now F_1 is a unique factorization domain implies that $F_2 = F_1[x_2] = F[x_1, x_2]$ is a unique factorization domain. Continuing this process a finite number of times, we conclude that $F[x_1, \ldots, x_n]$ is a unique factorization domain.

31 Eienstein's Criterion of Irreducibility

Theorem 1: *Let F be the field of quotients of a unique factorization domain R. If*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in R[x]$$

and p is a prime element of R such that

$$p \mid a_0,\ p \mid a_1,\ p \mid a_2, \ldots, p \mid a_{n-1}$$

whereas p is not a divisor of a_n and p^2 is not a divisor of a_0, then $f(x)$ is irreducible in $F[x]$.

(Gorakhpur 2011, 13)

Proof: Without loss of generality we may take $f(x)$ to be primitive, for taking out the greatest common factor of its coefficients does not disturb the hypothesis, since p is not a divisor of a_n. Now suppose that $f(x)$ is reducible in $F[x]$. Then $f(x)$ can be factored as the product of two polynomials of positive degree in $F[x]$. Therefore by Gauss lemma $f(x)$ can be factored as the product of two polynomials of positive degree in $R[x]$. Thus if we assume that $f(x)$ is reducible in $F[x]$, then

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_n x^n \\ &= (b_0 + b_1 x + \ldots + b_r x^r)(c_0 + c_1 x + \ldots + c_s x^s) \qquad \ldots(1) \end{aligned}$$

where the b's and c's are elements of R and where $r > 0$ and $s > 0$.

We have from (1), $a_0 = b_0\, c_0$.

Since p is a prime element of R, therefore

$$p \mid a_0 \Rightarrow p \mid b_0 \quad \text{or} \quad p \mid c_0.$$

Since p^2 is not a divisor of a_0, therefore p cannot divide both b_0 and c_0. Suppose that

$$p \mid b_0 \text{ and } p \text{ is not a divisor of } c_0.$$

If p is a divisor of all the coefficients $b_0, b_1, \ldots, b_r$, then from (1) we see that p is a divisor of all the coefficients of $f(x)$. But p is not a divisor of a_n. Therefore not all the coefficients $b_0, b_1, \ldots, b_r$ can be divisible by p. Let b_k, where $k \le r$, be the first b which is not divisible by p. Then each of $b_0, b_1, \ldots, b_{k-1}$ is divisible by p and b_k is not divisible by p.

Also $k < n$, since $r < n$.

Now from (1), we have

$$a_k = b_k c_0 + b_{k-1} c_1 + b_{k-2} c_2 + \ldots + b_0 c_k$$

$$\Rightarrow \quad b_k c_0 = a_k - b_{k-1} c_1 - b_{k-2} c_2 - \ldots - b_0 c_k . \qquad \ldots(2)$$

Now $k < n$. Therefore $p \mid a_k$. Also $p \mid b_{k-1}, b_{k-2}, \ldots, b_0$.

Therefore from (2), we have

$$p \mid b_k c_0 \quad \Rightarrow \quad p \mid b_k \text{ or } p \mid c_0 ,$$

since p is a prime element of R.

But this is nonsense because according to our initial assumptions p is neither a divisor of b_k nor a divisor of c_0. Hence $f(x)$ must be irreducible in $F[x]$. This completes the proof of the theorem.

Note: In the above theorem if we take the ring of integers **I** in place of the unique factorization domain R, then the field of quotients of **I** is the field of rational numbers. The statement of the theorem will be as follows :

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ *be a polynomial with integer coefficients. If p is a prime number such that*

$$p \mid a_0 , p \mid a_1, \ldots, p \mid a_{n-1}$$

whereas p is not a divisor of a_n *and* p^2 *is not a divisor of* a_0, *then* $f(x)$ *is irreducible over the field of rational numbers.*

There will be no difference in proof.

32 Fields of Rational Functions

Let $x, x_1, x_2, \ldots, x_n$ be indeterminates over an integral domain D. Then $D[x]$ and $D[x_1, x_2, \ldots, x_n]$ are integral domains. An element in the field of fractions of $D[x]$ is called a rational function in x over D. The field of fractions of $D[x]$ is called the field of rational functions over D in x and is denoted by $D(x)$. An element in the field of fractions of $D[x_1, x_2, \ldots, x_n]$ is called a rational function in $x_1, x_2, \ldots, x_n$ over D. The field of fractions of $D[x_1, x_2, \ldots, x_n]$ is called the field of rational functions over D in $x_1, x_2, \ldots, x_n$ and is denoted by $D(x_1, x_2, \ldots, x_n)$.

A rational function over D is a fraction $\frac{f}{g}$ of two polynomials over D such that $g \neq 0$. Two rational functions $\frac{f_1}{g_1}$ and $\frac{f_2}{g_2}$ are equal iff the two polynomials $f_1 g_2$ and $g_1 f_2$ are qual. The two rational functions $\frac{f_1}{g_1}$ and $\frac{f_2}{g_2}$ are added and multiplied

according to the following rules.

$$\frac{f_1}{g_1}+\frac{f_2}{g_2}=\frac{f_1g_2+g_1f_2}{g_1g_2} \text{ and } \frac{f_1}{g_1}\cdot\frac{f_2}{g_2}=\frac{f_1f_2}{g_1g_2}.$$

provided g_1 and g_2 are distinct from the zero polynomial over D.

Lemma 1: *If D be an integral domain, F the field of fractions of D and x be an indeterminate of D, then $D(x) = F(x)$.*

Proof: Here F consists of fractions $\frac{a}{b}$, such that $a, b \in D$ and $b \neq 0$. $D(x)$ consists of the fractions

$$\frac{a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0}{b_mx^m+b_{n-1}x^{m-1}+\ldots+b_1x+b_0},$$

such that $a_n, a_{n-1}, \ldots, a_1, a_0, b_m, b_{m-1}, \ldots, b_1, b_0 \in D$ and the denominator is distinct from the zero polynomial in $D[x]$.

$F(x)$ consists of the fractions $\frac{c_nx^n+c_{n-1}x^{n-1}+\ldots+c_1x+e_0}{d_mx^m+d_{m-1}x^{m-1}+\ldots+d_1x+d_0}$,

such that $c_n, c_{n-1}, \ldots, c_1, c_0, d_m, d_{m-1}, \ldots, d_1, d_0 \in F$ and the denominator is distinct from the zero polynomial in $F[x]$.

We have $D[x] \subseteq F[x]$, as an element of D is identified with the fraction $\frac{a}{1}$ in F, where $D \subseteq F$.

Note that the two elements $\frac{f_1(x)}{g_1(x)}$ and $\frac{f_2(x)}{g_2(x)}$ of $D(x)$ are equal in $D(x)$ iff

$$f_1(x)\ g_2(x) = g_1(x)\ f_2(x) \text{ in } D[x],$$

and this holds iff $f_1(x)\ g_2(x) = g_1(x)\ f_2(x)$ in $F[x]$ that is iff $\frac{f_1(x)}{g_1(x)}$ and $\frac{f_2(x)}{g_2(x)}$ are equal in $F(x)$.

Therefore, every element of $D(x)$ is in $F(x)$ and equality of $D(x)$ coincides with equality in $F(x)$. Thus,

$$D(x) \subseteq F(x).$$

To show $F(x) \subseteq D(x)$.

Let $\frac{f_2(x)}{g_2(x)} \in F(x)$, such that $f_2(x), g_2(x) \in F[x]$, $g(x) \neq 0$.

We have

$$f_2(x)=\sum_{i=0}^{n}\frac{a_i}{b_i}x^i,\ g_2(x)=\sum_{j=0}^{m}\frac{c_j}{d_j}x^j,$$

such that $a_i, b_i, c_j, d_j \in D, b_i \neq 0, d_j \neq 0$ for all i, j and not all of c_j are equal to $0 \in D$. Putting $b = b_0b_1 \ldots b_{n-1}b_n$ and $d = d_0d_1 \ldots d_{m-1}d_m$, we have $dbf_2(x)$ and $dbg_2(x)$ as polynomials in $D[x]$.

$\therefore \quad \dfrac{f_2(x)}{g_2(x)} = \dfrac{dbf_2(x)}{dbg_2(x)} \in D(x).$

Thus $F(x) \subseteq D(x)$.

Hence $D(x) = F(x)$.

Illustration: $\dfrac{\frac{1}{3}x^2 - \frac{1}{7}x + \frac{1}{4}}{\frac{1}{5}x^2 + \frac{1}{3}x + \frac{1}{2}} \in Q(x)$

is equal to the rational function $\dfrac{5(28x^2 - 12x + 21)}{14(6x^2 + 10x + 15)}$ in $Z[x]$.

Remark: If D be an integral domain and F the field of fractions of D, then

$$\begin{aligned} D(x_1, x_2, \ldots, x_n) &= \text{field of fractions of } D[x_1, x_2, \ldots, x_n] \\ &= \text{field of fractions of } D[x_1, x_2, \ldots, x_{n-1}][x_n] \\ &= D(x_1, x_2, \ldots, x_{n-1})(x_n) \end{aligned}$$

Putting $n = 1$ in the lemma 1, we have

$$D(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n),$$

that is the result is true for $n = 1$.

If it is true for $n = k$, that is

$$D(x_1, x_2, \ldots, x_k) = F(x_1, x_2, \ldots, x_k)$$

it is also true for $n = k + 1$, as

$$\begin{aligned} D(x_1, x_2, \ldots, x_k, x_{k+1}) &= D(x_1, x_2, \ldots, x_k)(x_{k+1}) \\ &= F(x_1, x_2, \ldots, x_k)(x_{k+1}) \\ &= F(x_1, x_2, \ldots, x_k, x_{k+1}). \end{aligned}$$

[Putting F in place of D and $k + 1$ in place of n in the Remark.]

Lemma 2: *Let $f(x)$ be a non-zero polynomial in $D[x]$, where D is a field. Also let $p(x)$ and $q(x)$ be two non-zero, relatively prime polynomials of positive degree in $D[x]$. If $f(x)$ is relatively prime to $p(x)\,q(x)$ and deg $f(x) <$ deg $p(x)\,q(x)$, then there exist uniquely determined non-zero polynomials $a(x), b(x)$ in $D[x]$, such that*

$$a(x)\,q(x) + b(x)\,p(x) = f(x),$$

deg $a(x) <$ deg $p(x)$

and *deg $b(x) <$ deg $q(x)$.*

Lemma3: *If D be a field and $\dfrac{f(x)}{g(x)}$ be a non-zero rational function in $D(x)$, such that deg $f(x) <$ deg $g(x)$, where $f(x)$ and $g(x)$ are both monic and $f(x)$ is relatively prime to $g(x)$. If $g(x) = p(x)\,q(x)$ such that $p(x), q(x)$ are relatively prime polynomials of positive degree in*

$D[x]$, then there exist uniquely determined non-zero polynomials $a(x)$ and $b(x)$ in $D[x]$, such that

$$\frac{f(x)}{g(x)} = \frac{f(x)}{p(x)\,q(x)} = \frac{a(x)}{p(x)} + \frac{b(x)}{q(x)},$$

$$\deg a(x) < \deg p(x)$$

and $$\deg b(x) < \deg q(x).$$

Lemma 4: *If D be a field and $\frac{f(x)}{g(x)}$ be a non-zero rational function in $D(x)$, such that $\deg f(x) < \deg g(x)$, where $f(x)$ and $g(x)$ are both monic and $f(x)$ is relatively prime to $g(x)$. If $g(x) = p_1(x)\,p_2(x)\ldots p_m(x)$ such that $p_1(x), p_2(x), \ldots, p_m(x)$ are pairwise relatively prime monic polynomials of positive degree in $D[x]$, then there exist uniquely determined non-zero polynomials $a_1(x), a_2(x), \ldots, a_m(x)$ in $D[x]$, such that*

$$\frac{f(x)}{g(x)} = \frac{f(x)}{p_1(x)\,p_2(x)\ldots p_m(x)} = \frac{a_1(x)}{p_1(x)} + \frac{a_2(x)}{p_2(x)} + \ldots + \frac{a_m(x)}{p_m(x)}$$

and $$\deg a_i(x) < \deg p_i(x) \quad \forall \quad i = 1, 2, \ldots, m.$$

Lemma 5: *Let x be an indeterminate over D and $g(x)$ be a polynomial in $D[x]$ of degree ≥ 1. Then for any $f(x) \in D[x]$ there exit uniquely determined polynomials $q_0(x), q_1(x), q_2(x), \ldots, q_n(x)$ such that*

$$f(x) = q_0(x) + q_1(x)\,g(x) + q_2(x)\,g(x)^2 + \ldots + q_n(x)\,g(x)^n$$

and $$q_i(x) = 0 \text{ or } \deg q_i(x) < \deg g(x) \quad \forall \quad i = 1, 2, \ldots, n.$$

Note: The unique expression $f = q_0 + q_1 g + q_2 g^2 + \ldots + q_n g^n$, where $q_i(x) = 0$ or $\deg q_i < \deg g \ \forall\ i = 1, 2, \ldots, n$ is called the g-adic expansion of f.

Theorem: *Let D be a field and $\frac{f(x)}{g(x)}$ a non-zero rational function in $D(x)$ such that $f(x),\ g(x) \in D[x]$ are relatively prime in $D[x]$. Let u be the leading coefficient of $g(x)$ and let $g(x) = u\,p_1(x)^{n_1}\,p_2(x)^{n_2}\ldots p_m(x)^{n_m}$ be the decomposition of $g(x)$ into polynomials irreducible over D, where $p_i(x)$ are monic. Then there exist uniquely determined polynomials $G(x), a_1^{(1)}(x), a_2^{(1)}(x), \ldots, a_{n_1}^{(1)}x, a_1^{(2)}(x), a_2^{(2)}(x), \ldots, a_{n_2}^{(2)}(x), \ldots, a_1^{(m)}(x), a_2^{(m)}(x), \ldots, a_{n_m}^{(m)}(x)$ in $D[x]$, such that*

$$\frac{f(x)}{g(x)} = G(x) + \frac{a_1^{(1)}(x)}{p_1^1(x)} + \frac{a_2^{(1)}(x)}{p_1^2(x)} + \ldots + \frac{a_{n_1}^{(1)}(x)}{p_1^{n_1}(x)} + \frac{a_1^{(2)}(x)}{p_2^1(x)} + \frac{a_2^{(2)}(x)}{p_2^2(x)} + \ldots$$
$$+ \frac{a_{n_2}^{(2)}(x)}{p_2^{n_2}(x)} + \ldots + \frac{a_1^{(m)}(x)}{p_m^1(x)} + \frac{a_2^{(m)}(x)}{p_m^2(x)} + \ldots + \frac{a_{n_m}^{(m)}(x)}{p_m^{n_m}(x)}$$

and deg $a_i^{(k)}(x) \leq \deg p_k(x)$ *or* $a_i^{(k)}(x) = 0 \quad \forall \quad i$ *and* k.

Proof: Dividing $f(x)$ by $g(x)$, we get unique polynomials $G(x)$, $H(x)$ in $D[x]$ such that

$$f(x) = g(x)\, G(x) + H(x),$$
$$\deg H(x) < \deg\ g(x) \ \text{ or } \ H(x) = 0.$$

If $H(x) = 0$, everything is proved as

$$a_i^{(k)}(x) = 0 \ \forall\ i \text{ and } k.$$

If $H(x) \neq 0$, let the leading coefficient of $H(x)$ be v. Put $c = v / u$. Since $f(x)$ and $g(x)$ are relatively prime, therefore $H(x)$ and $g(x)$ are relatively prime.

We have $H(x) = v\,h(x)$, where $h(x)$ is monic and relatively prime to $g(x)$ and

$$\frac{f(x)}{g(x)} = G(x) + c\,\frac{h(x)}{g(x)}$$

such that $\deg\ h(x) < \deg\ g(x)$.

Using Lemma 4, we get uniquely determined non-zero polynomials $b_1(x)$, $b_2(x), \ldots, b_m(x)$ in $D[x]$ such that

$$\frac{f(x)}{g(x)} = \frac{b_1(x)}{p_1(x)^{n_1}} + \frac{b_2(x)}{p_2(x)^{n_2}} + \ldots + \frac{b_m(x)}{p_m(x)^{n_m}}$$

and $\quad \deg\ b_k(x) < \deg\ p_k(x)^{n_k} \quad \forall \quad k = 1, 2, \ldots, m.$

Putting $f_k(x) = c b_k(x)$, we get

$$\frac{f(x)}{g(x)} = G(x) + \frac{f_1(x)}{p_1(x)^{n_1}} + \frac{f_2(x)}{p_2(x)^{n_2}} + \ldots + \frac{f_m(x)}{p_m(x)^{n_m}}.$$

Since c is uniquely determined by $f(x)$ and $g(x)$, the polynomials $f_k(x)$ are also uniquely determined.

Since $\quad \deg\ f_k(x) = \deg\ b_k(x) < \deg\ p_k(x)^{n_k}$,

in the $p_k(x)$-adic expansion

$$f_k(x) = q_0(x) + q_1(x)p_k(x) + q_2(x)p_k(x)^2 + \ldots + q_s(x)p_k(x)^s,$$

the polynomials $q_t(x) = 0$ for $t \geq n_k$.

Let $\quad f_k(x) = a_1^{(k)}(x)\ p_k(x)^{n_k - 1} + a_2^{(k)}(x)\, p_k(x)^{n_k - 2} + \ldots$

$$+ a_{n_k - 1}^{(k)}(x)\, p_k(x) + a_{n_k}^{(k)}(x)$$

be the $p_k(x)$-adic expansion of $f_k(x)$.

The polynomials $a_1^{(k)}, a_2^{(k)}, \ldots, a_{n_k}^{(k)}$ in $D[x]$ are uniquely determined and

$$\deg a_i^{(k)} < \deg\ p_k(x)$$

or $\quad a_i^{(k)} = 0 \quad \forall \quad i = 1, 2, \ldots, n_k$.

Thus for all $k = 1, 2, \ldots, m$, we have

$$\frac{f_k(x)}{p_k(x)^{n_k}} = \frac{a_1^{(k)}(x)}{p_k^1(x)} + \frac{a_2^{(k)}(x)}{p_k^2(x)} + \ldots + \frac{a_{n_k}^{(k)}(x)}{p_k^{n_k}(x)}.$$

Hence, the theorem is proved.

The equation

$$\frac{f(x)}{g(x)} = G(x) + \frac{a_1^{(1)} x}{p_1{}^1(x)} + \frac{a_2^{(1)}(x)}{p_1{}^2(x)} + \ldots + \frac{a_{n_1}^{(1)}(x)}{p_1{}^{n_1}(x)} + \frac{a_1^{(2)}(x)}{p_2{}^1(x)} + \frac{a_2^{(2)}(x)}{p_2{}^2(x)} + \ldots + \frac{a_{n_2}^{(2)}(x)}{p_2{}^{n_2}(x)} + \ldots + \frac{a_1^{(m)}(x)}{p_m{}^1(x)} + \frac{a_2^{(m)}(x)}{p_m{}^2(x)} + \ldots + \frac{a_{n_m}^{(m)}(x)}{p_m{}^{n_m}(x)}$$

is called the expansion of $\frac{f(x)}{g(x)}$ in partial fractions.

Comprehensive Exercise 2

1. If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the field of rational numbers. **(Gorakhpur 2013)**
2. Show that the polynomial $x^2 - 3$ is irreducible over the field of rational numbers.
3. Prove that the polynomial $1 + x + \ldots + x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers.
4. Show that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible over the field of rational numbers.
5. Let R be a unique factorization domain. Then show that every prime element in R generates a prime ideal.

Objective Type Questions

Multiple Choice Questions

Indicate the correct answer for each question by writing the corresponding letter from (a), (b), (c) *and* (d).

1. If F is a field and $f(x)$, $g(x)$ are two non-zero elements of $F[x]$, then $\deg[f(x)\,g(x)] =$
 (a) $\deg f(x) + \deg g(x)$ (b) $\deg f(x) - \deg g(x)$
 (c) $\deg f(x) \cdot \deg g(x)$ (d) none of these
2. The polynomial $x^2 + 1$ is reducible over the field of
 (a) rational numbers (b) real numbers
 (c) complex numbers (d) one of these

3. If $f(x) \in F[x]$ and $a \in F$, for a field F, then $(x - a)$ divides $f(x)$ if and only if
 (a) $f(a) = 0$ (b) $f(a) \neq 0$
 (c) $f'(a) = 0$ (d) $f'(a) \neq 0$
4. Let $f(x) = 2 + 6x + 4x^2$, $g(x) = 2x + 4x^2$ be two polynomials over the ring $(\mathbf{I}_8, +_8, \times_8)$. Then deg $[f(x) + g(x)]$ is
 (a) 0 (b) 1
 (c) 2 (d) 4
5. Let R be a Euclidean ring. Let a and b be two non-zero elements in R. Then if b is a unit in R,
 (a) $d(ab) > d(a)$ (b) $d(ab) < d(a)$
 (c) $d(ab) = d(a)$ (d) none of these.
6. The necessary and sufficient condition that the non-zero element a in the Euclidean ring R is a unit is that
 (a) $d(a) > d(1)$ (b) $d(a) < d(1)$
 (c) $d(a) = d(1)$ (d) none of these.

Fill in the Blank(s)

Fill in the blanks "……", so that the following statements are complete and correct.

1. If R is an arbitrary ring and R' is the set of constant polynomials in $R[x]$, then R' is …… to R.
2. Two polynomials $f(x)$ and $g(x) \in F[x]$ are said to be …… if their greatest common divisor is 1, the unity element of the field F.
3. If $f(x) \in F[x]$ and $a \in F$, for any field F, then …… is the remainder when $f(x)$ is divided by $(x - a)$.
4. An ideal S of the ring of integers $\mathbf{I}$ is maximal if and only if S is generated by some …… integer.
5. Every Euclidean ring is a …… ring.
6. Every Euclidean ring possesses …… element.

True or False

Write 'T' for true and 'F' for false statement.

1. The polynomial domain $F[x]$ over a field F is a field.
2. The polynomial ring $\mathbf{I}[x]$ over the ring of integers is not a principal ideal ring.
3. The field of real numbers is a prime field.
4. A Euclidean ring is a unique factorization domain.
5. The ring of Gaussian integers is not a Euclidean ring.
6. Every field is a Euclidean ring.

Answers

Multiple Choice Questions

1. (a) **2.** (c) **3.** (a) **4.** (a) **5.** **(c)**
6. (c)

Fill in the Blank(s)

1. isomorphic **2.** relatively prime **3.** $f(a)$
4. prime **5.** principal ideal **6.** unity

True or False

1. *F* **2.** *T* **3.** *F* **4.** *T* **5.** *F*
6. *T*

□